# PERSONAL DATA PROTECTION POLICY & PROCEDURES

| POLICY DOCUMENT INFORMATION | |
|---|---|
| **Policy Document Category:** | University Wide |
| **Policy Document Owner:** | Office of Risk Management and Compliance |
| **Applies:** | University wide - All Staff and Students<br><br>*Volunteers, agents, contractors, consultants, contract workers, vendors and any other persons engaged/hired by a Staff/Student of the University are also required to comply with this Policy Document and Staff/Students engaging/hiring such individuals shall be responsible for ensuring such compliance. |
| **Effective Date:** | 5 April 2022 |

**POLICY DOCUMENT HISTORY**

| **Version No.** | **Approved by** (Name, Designation) | **Approval Date** | **Effective Date** | **Policy Document Change** |
|---|---|---|---|---|
| V1 | John Wilton | 23 June 2020 | 28 Aug 2020 | New Document |
| V2 | Prof Tan Eng Chye | 5 April 2022 | 5 April 2022 | Major Amendments |

| SUPERSEDED POLICY DOCUMENTS | |
|---|---|
| **Name of superseded Policy Document** | PDPA Compliance Guidelines<br><br>Do-Not-Call Policy and Procedures |

# CONTENTS

## 1 DEFINITIONS & INTERPRETATION

Please refer to Appendix 1 for the definition of the various capitalised terms used in this Personal Data Protection Policy ("**Policy Document**").

## 2 RATIONALE & OBJECTIVES

2.1 Rationale:

2.1.1 In recognition of the importance of all Personal Data entrusted to it, NUS believes that it is its responsibility to properly manage, protect and process such Personal Data and is fully committed to the University's compliance with the PDPA.

2.1.2 Given the significance of Personal Data and the complexity of University operations, the University needs clear policies and procedures in place in order:

(i) to safeguard such data while still ensuring its availability for all functional units who require access to such data; and

(ii) for efficient and effective business processing and decision-making to take place when managing and using such data.

2.2 Objectives:

The principal objectives of this Policy Document is to:

(i) lay down the general principles and obligations that Staff/Students have to comply with when handling Personal Data;

(ii) ensure clear accountability for individual roles involved in the process;

(iii) ensure that the data protection rights of Staff/Students and other individuals who have provided Personal Data to NUS are safeguarded; and

(iv) minimise the risk of NUS being subject to the adverse consequences that can arise from any breach of the PDPA (e.g. the PDPC imposing financial penalties of up to S$1 million or 10% of annual turnover in Singapore (whichever is higher) and/or issuing directions to stop NUS from continuing certain activities, civil/criminal liability, significant time, resources and management input being expended during investigations, disruption to business/operations, negative impact on NUS' general reputation etc.).

## 3 SCOPE

3.1 The policy statements set out in this Policy Document apply to:

(i) all units within NUS and their Staff and Students;

(ii) and all Personal Data that Staff/Students collect, use and/or disclose, in the course of their daily operational activities for NUS and/or in the course of their employment), including but not limited to Personal Data relating to:

(a) NUS Staff & Students – current, incoming or potential (e.g. employment candidates);

(b) NUS' alumni;

(c) actual or potential providers for goods or services (including tender applicants), or their employees, agents, representatives or contractors; and

(d) persons otherwise engaged in, associated with, or affected by the operations of NUS.

3.2 All volunteers, agents, contractors, consultants, contract workers, vendors and any other persons engaged/hired by a Staff/Student of the University are also required to comply with this Policy and Staff/Students engaging/hiring such individuals shall be responsible for ensuring such compliance.

## 4 INTERFACE WITH THE NUS DATA MANAGEMENT POLICY & RELATED POLICIES

4.1 The management and treatment of all University Data (of which Personal Data forms part) is governed by, *inter alia*:

(i) all Policy Documents relating to the management of University Data that may be issued by NUS IT from time to time, including, but not limited to:

(a) the Acceptable Use Policy for IT Resources ("**AUP**") and AUP Guidelines;

(b) the Cloud Policy;

(c) the DMP and DMP Appendices;

(d) the NUS Guidelines on Use Classification and Protection of University Data;

(e) Guidelines for Personal Computers & Equipment

(f) the IT Security Policy;

(g) Mobile Device Security Policy;

(h) Software Management Policy;

(i) Software terms of use;

(collectively, the "**NUS IT Policy Documents**");

(ii) for Research Data only - all NUS Policy Documents relating to the management of Research Data, including but not limited to:

(a) the NUS Research Data Management Policy; and

(b) the NUS Code & Procedures for Research Integrity;

(c) (collectively, the "**Research Data Policy Documents**"); and

(d) any other NUS Policy Documents relating to the management and treatment of University Data (including such additional Policy Documents as the University may from time to time issue).

4.2 Where any University Data consists of Personal Data, then, **in addition** to the obligations set out in the documents listed in paragraph 4.1 above, the requirements set out in this Policy Document must also be adhered to.

4.3 For the avoidance of doubt, when handling any Personal Data that falls within the definition of University Data (as defined in the DMP), Staff and Students must adhere to the requirements set out in:

(i) this Personal Data Protection Policy & Procedures;

(ii) the NUS IT Policy Documents;

(iii) the Research Data Policy Documents (if applicable); and

(iv) any other NUS Policy Documents relating to the management and treatment of University Data (including such additional Policy Documents as the University may from time to time issue)

## 5 EU GENERAL DATA PROTECTION REGULATION (GDPR)

5.1 In carrying out its activities, NUS handles a limited volume of Personal Data which is subject to European data protection rules. As such, NUS must have regards to these rules when handling such data.

5.2 The General Data Protection Regulation ("**GDPR**") sets out the rules applicable to the collection, processing and storage of the Personal Data of individuals located in the European Economic Area.

5.3 GDPR requirements overlap with PDPA requirements in a number of ways, but contain additional requirements which are not addressed in the PDPA. As such, where NUS is handling Personal Data which is subject to European data protection rules, it needs to ensure that it complies with these additional GDPR requirements.

5.4 For a summary of GDPR requirements, please refer to Appendix 20. All Staff/Students must review those requirements and comply with them any time they are handling Personal Data which is subject to European data protection rules.

# A. POLICY STATEMENTS

## 6 REQUIREMENTS UNDER THE PDPA

The PDPA contains the following 2 sets of requirements:

(i) Personal Data protection requirements; and

(ii) Do-Not-Call ("**DNC**") Registry requirements.

## 7 WHAT IS PERSONAL DATA UNDER THE PDPA?

7.1 Definition:

"**Personal Data**" is defined under the PDPA to mean:

(i) data, whether true or not, about an individual who can be identified: from that data;

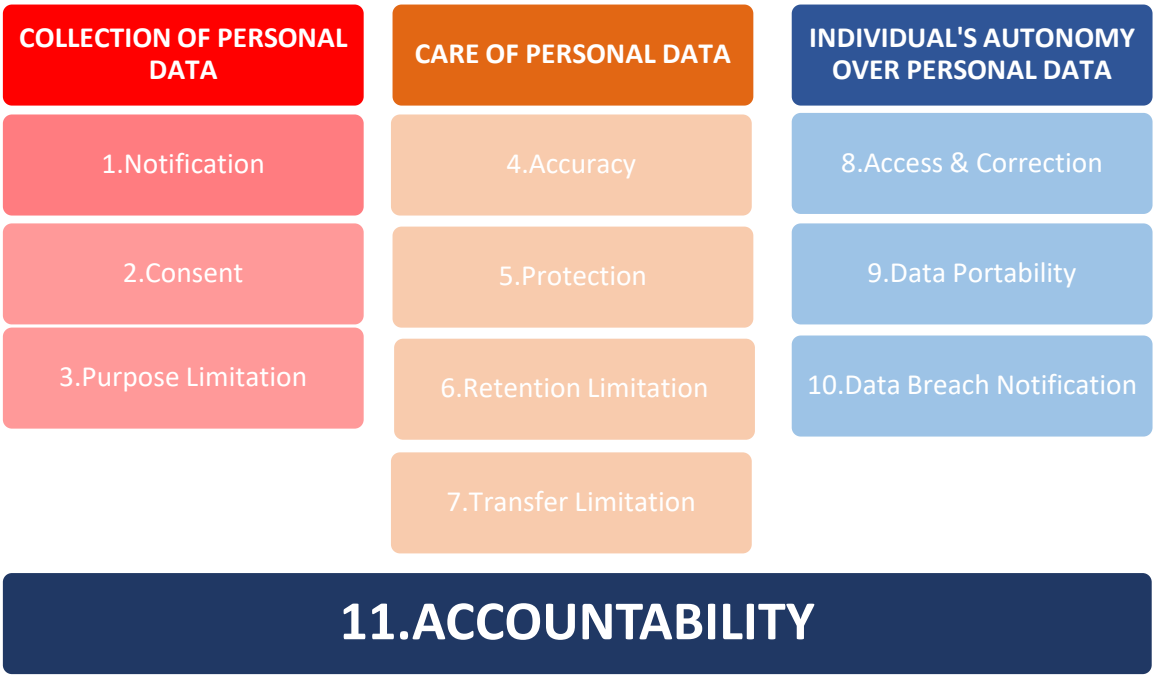
(ii) or from that data and other information to which an organization has or is likely to have access.

7.2 For further details on what constitutes Personal Data, please refer to Appendix 2 and 3.

## 8 PERSONAL DATA PROTECTION OBLIGATIONS UNDER THE PDPA

8.1 Obligations of Staff/Students under the PDPA:

When dealing with the Personal Data of any individuals, all Staff and Students must adhere to the following 11 data protection principles:




## 9 COLLECTION OF PERSONAL DATA

9.1 Notification Obligation

Staff/Students must notify an individual of the purposes for which they are intending to collect, use or disclose his/her Personal Data on or before the collection, use or disclosure of Personal Data.

9.2 Consent Obligation

Staff/Students must:

(i) only collect, use or disclose Personal Data for purposes which an individual has given his consent (whether express or deemed);

(ii) allow the individual to withdraw consent; and

(iii) upon withdrawal of consent, cease such collection, use or disclosure.

9.3 Purpose Limitation Obligation

Staff/Students:

(i) can only collect, use or disclose Personal Data about an individual for the purposes for which the individual has given consent (whether express or deemed); and

(ii) must limit their collection, use or disclosure of the individual's personal data only to such purposes.

## 10 CARE OF PERSONAL DATA

10.1 Accuracy Obligation

Staff/Students must take reasonable efforts to ensure that Personal Data collected by or on their behalf is accurate and complete, especially if it is likely to be used to make a decision that affects the individual, or if it is likely to be disclosed to another organisation.

10.2 Protection Obligation

10.2.1 Staff/Students must take reasonable security measures to protect the Personal Data of individuals that is in their possession or control, in order to prevent unauthorised access, use, disclosure or similar risks.

10.2.2 Staff/Students who engage a Data Intermediary to process Personal Data on their behalf must ensure that the data intermediary adheres to the Protection obligations.

10.3 Retention Limitation Obligation

10.3.1 Staff/Students must cease retention or remove the means by which the Personal Data can be associated with particular individuals when:

(i) it is reasonable to assume that the purpose for initially collecting the Personal Data is no longer required; and

(ii) there is no legal or business purpose for retaining the Personal Data.

10.3.2 Staff/Students who engage a Data Intermediary to process Personal Data on their behalf must ensure that the Data Intermediary adheres to the Retention Limitation obligations.

10.4 Transfer Limitation Obligation

Staff/Students must only transfer Personal Data to a country outside Singapore in accordance with the requirements prescribed under the PDPA, namely:

(i) take appropriate steps to ensure that NUS will continue to comply with the PDPA in respect of the transferred Personal Data while it remains in the possession or under the control of NUS; and

(ii) take appropriate steps to ascertain whether and ensure that the recipient of the Personal Data overseas is bound by legally enforceable obligations to provide to the Personal Data transferred a standard of protection that is comparable to that under the PDPA.

10.5 Access and Correction

Staff/Students must, upon request:

(i) provide an individual with the Personal Data and information about the ways in which his/her Personal Data has been or may have been used or disclosed within 1 year before the request; and

(ii) correct any error or omission in an individual's Personal Data and send the corrected data to other organisations to which the Personal Data was disclosed by NUS within 1 year before the correction is made.

10.6 Data Portability:

Staff/Students must, upon request of individuals that have an existing direct relationship with NUS transmit the individual's Personal Data (that is in an electronic form) and in NUS' control/possession, to another organisation with a presence in Singapore in a commonly used machine-readable format.

## 11 ACCOUNTABILITY OBLIGATION

Staff/Students must:

(i) adhere to the PDPA data obligations and NUS' data protection policies and practices; and

(ii) act on feedback from our various stakeholders.

## 12 IMPLEMENTATION & APPLICATION REQUIREMENTS

For further details on the steps/processes to be followed/taken by Staff and Students in relation to their compliance with the abovementioned obligations of the PDPA, please refer to the following Appendices:

(i) Appendix 4 – Consent Obligation

(ii) Appendix 5 – Purpose Limitation Obligation

(iii) Appendix 6 – Notification Obligation

(iv) Appendix 7 – Accuracy Obligation

(v) Appendix 8 – Protection Obligation

(vi) Appendix 9 – Retention Limitation Obligation

(vii) Appendix 10 – Transfer Limitation Obligation

(viii) Appendix 11 – Access & Correction Obligation

(ix) Appendix 12 – Data Breach Notification Obligation

(x) Appendix 13 – Accountability Obligation

## 13 THE DO-NOT-CALL (DNC) OBLIGATIONS

Where marketing messages to Singapore telephone numbers via voice/phone calls, SMS/MMS (text messages) or fax are intended to be sent out, Staff/Students will be required to comply with the provisions relating to the DNC regime. NUS' policy for compliance with the DNC regime is set out in NUS' Do Not Call Policy and Procedures in Appendix 14 below.

## 14 EXCLUSIONS AND EXCEPTIONS TO THE OBLIGATIONS UNDER THE PDPA

There are limited exclusions and exceptions under the PDPA pertaining to very specific scenarios, circumstances and/or conditions whereby one or more of the data protection principles would not apply. For further details of such exclusions and exceptions, please see Appendix 15 below.

## 15 ENGAGEMENT WITH THIRD PARTIES

15.1 When engaging with third parties, Staff/students must ensure that if their dealings with such third parties involve Personal Data, they must be mindful of and ensure compliance under the PDPA in the course of such dealings.

15.2 For further details on the considerations that Staff/Students must bear in mind when interacting with third parties, please refer to Appendix 16.

## 16 PERSONAL DATA OF NUS STAFF AND STUDENTS

16.1 NUS collects, uses and discloses the Personal Data of NUS Staff and Students for the purposes listed in the Employee Personal Data Notice and Consent Statements or Student Personal Data Notice and Consent Statements respectively which were sent by the Circular dated 30 June 2014 (as the same may be amended/revised, updated and/or supplemented from time to time) and which Staff/Students have agreed to and accepted as part of their employment/enrolment with NUS. These statements can be found for Staff at the NUS Staff Portal and for Students at the NUS Student Portal.

16.2 For further details on how NUS protects, administers and manages the Personal Data of Staff/Students, please refer to Appendix 17.

---

# B. PROCEDURES

---

## 17 ROLES AND RESPONSIBILITIES

The roles and responsibilities of the relevant parties in the University's Data Protection Framework are set out in Appendix 18 below

## 18 DATA BREACH

For further details on what constitutes a Data Breach and the Data Breach management requirements to be adhered to by Staff/Students, please refer to Appendix 12.

## 19 COMPLAINTS

Staff/Students who are aware of an individual wishing to make a complaint please inform the Data Protection Office immediately at dpo@nus.edu.sg.

## 20 POLICE INVESTIGATIONS/RAIDS

In the event that representatives of the PDPC arrive at NUS for an investigative purpose, Staff/Students must adhere to the procedures set out in Appendix 19.

---

# C. GENERAL

---

## 21 REVIEW OF POLICY

21.1 This Policy Document shall be reviewed by the Policy Document Owner in accordance with the requirements set out in the University's Policy on Policies, or more frequently if deemed necessary by the Policy Document Owner. Any recommendation for changes to this Policy Document (whether amendments, repeal or otherwise) must similarly be carried out in accordance with the requirements of the Policy on Policies.

21.2 The University shall be entitled to revise, amend or update this Policy Document and to issue additional Policy Documents from time to time. All such revisions, amendments, updates and additions shall be deemed to be a part of this Policy Document. Any revisions, amendments, updates or additions to this Policy Document issued by the University may be published or notified through written notice, electronic mail, the University website, or such other form of communication as the University may deem appropriate.

## 22 QUERIES

All questions as to the interpretation of this Policy Document shall be referred to the Policy Document Contact.

## 23 INTERPRETATION

23.1 Headings

The headings of the provisions of this Policy Document are to facilitate reference only and do not form a part of this Policy Document, and shall not in any way affect the construction or interpretation thereof.

23.2 Inconsistency with this Policy Document

In the event of any inconsistency between the requirements set out in this Policy Document and those set out in any other Policies, Procedures, Guidelines or other documents relating to the subject matter of this Policy Document, the requirements set out in this Policy Document shall prevail unless otherwise stated.

## 24 ADHERENCE TO POLICY DOCUMENT

24.1 Compliance with this Policy Document is mandatory and any failure to comply with this Policy Document (including any arrangements that are established under it) may, at the University's absolute discretion, be investigated and result in such corrective and/or disciplinary action(s) as the University deems fit.

24.2 Units must ensure that as soon as it reasonably suspects a breach of the provisions of this Policy Document, it shall:

(i) inform the Data Protection Office; and

(ii) when further investigation is required, in line with the Staff Disciplinary Procedures & Sanctions or its Student equivalent as embedded in NUS' Statute and Regulations, the responsible unit will consult with the DPO as subject matter expert on the further investigation, the requirements thereof and analysis of the evidence.

## 25 EXCEPTIONS TO THIS POLICY DOCUMENT

Any exceptions to the requirements of this Policy Document requires prior written approval from:

(i) For University-wide Policy Documents - President (or such other appropriate senior management personnel as the President may from time to time designate);

(ii) For Academic/Administrative/Innovation & Enterprise/Research & Technology categories - Cluster Head of the Policy Owner;

and such approval will only be granted in very exceptional circumstances.

## APPENDIX 1- DEFINITIONS

IN THIS PERSONAL DATA PROTECTION POLICY & PROCEDURES (THIS "POLICY DOCUMENT"), THE FOLLOWING WORDS SHALL HAVE THE FOLLOWING MEANINGS:

| | |
|---|---|
| **"Data Breach"** | In relation to Personal Data, refers to:<br><br>(i) the unauthorised access, collection, use, disclosure, copying, modification or disposal of Personal Data; or<br><br>(ii) the loss of any storage medium or device on which Personal Data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the Personal Data is likely to occur. |
| **"Data Protection Office"** | The NUS Data Protection Office |
| **"Data Subject"** | Refers to any person whose personal data is being collected, held or processed |
| **"Dean"** | Refers to the Dean of a Faculty, School or Programme. |
| **"DMP"** | The NUS Data Management Policy 3.0, as the same may be amended/revised and/or supplemented from time to time. |
| **"DMP Appendices"** | The NUS Data Management Policy 3.0 Appendices, as the same may be amended/revised and/or supplemented from time to time. |
| **"DPO"** | The NUS Data Protection Officer |
| **"Head"** | "Head" includes the Head of an academic Department or Director of an administrative office, institute, centre, unit or other subdivisions of teaching, research and administration. In the event that either the Head of an Academic Unit and the Dean of the corresponding Faculty, School or Programme are one and the same person, or a Faculty, School or Programme consists of only one Academic Unit or no Academic Units, the Dean of the corresponding Faculty shall designate one of the Vice Deans (or a person holding an equivalent position) as the "Head". The designated Head shall be conferred all the powers exercisable by the Head of an Academic Unit under these procedures and for such period and subject to such conditions as the Dean may deem fit. |
| **"Law"** | Refers to all applicable laws relevant to this Policy including but not limited to Singapore law. This shall include, but is not limited to, any and all existing legislation in Singapore, any and all rules, regulations, codes of practice, by-laws, ordinances, decrees, practice directions, standards of performance and any other requirements imposed by any Governmental Authority, and all amendments and/or revisions thereto from time to time. |
| **"NUS" or the "University"** | The National University of Singapore and/or any of its Departments |
| **"OLA"** | Office of Legal Affairs |

| | |
|---|---|
| **"PDPA"** | Refers to the Singapore Personal Data Protection Act 2012, as the same may be amended, revised and/or re-enacted thereto from time to time |
| **"PDPA Legislation"** | Refers to the Singapore Personal Data Protection Act 2012, including all subsidiary legislations, re-enactments, supplements, amendments and any advisory and guidelines issued by the Singapore Personal Data Protection Commission, as the same may be amended, revised and/or re-enacted thereto from time to time<br>. |
| **"PDPA POC"** | Refers to Personal Data Protection Point of Contact<br><br>For further details, please refer to Appendix 18 below. |
| **"PDPC"** | Personal Data Protection Commission |
| **"Personal Data"** | Where the word "Personal Data" is used in or in connection with or in relation to this Policy Document or any matter addressed herein, it shall have the meaning ascribed to it in the PDPA (as the same may be amended and/or revised thereto from time to time), paragraph 7 of this Policy Document and as further described in Appendices 2 and 3. |
| **"Policy Document(s)"** | University document, which is employed in the governance and administration of the University's operations (i.e. Policies, Procedures and Guidelines and such other documents as management may from time to time designate as such). |
| **"Research Data"** | As defined in the NUS Research Data Policy Documents |
| **"Staff"** | Refers to all NUS full-time or part-time Academic, non-Academic and Executive and Professional employees. |
| **"Student"** | As defined in the NUS Statutes and Regulations. |
| **"University Data"** | As defined in the DMP |

**INTERPRETATION**

1.1. The word 'may' when used to bestow a duty or power indicates that the action or decision may be enacted or not, at discretion.

1.2. For the avoidance of doubt, the words 'must', 'shall' or 'will', if used to bestow a duty or power, indicate that the action or decision is mandatory and must be enacted.

1.3. A reference to the word 'including' in any form is not to be construed or interpreted as a word of limitation.

## APPENDIX 2 - PERSONAL DATA

### 1 PERSONAL DATA:

(i) can both electronic and non-electronic data

(ii) can be factual or an opinion

### 2 EXAMPLES OF PERSONAL DATA:

2.1 By way of illustration, examples of Personal Data include (but are not limited to) the following:

(i) Individual's name

(ii) NRIC number, FIN (Foreign Identification Number), passport numbers and other national identification numbers (see paragraph 2.2)

(iii) contact details such as residential address (see paragraph 2.3), personal phone number, personal email address

(iv) medical records

(v) biometric information (see paragraph 2.4) (e.g. fingerprint, iris image, DNA profile, voice recording) and research data (see paragraph 2.5)

(vi) facial image of an individual (e.g. photograph / video recording)

(vii) employment appraisal or evaluation

(viii) a reference about an individual

2.2 NRIC and other national identification numbers:

The PDPC has issued guidelines governing the:

(i) collection, use and disclosure of national identification numbers (e.g. NRIC numbers, passport numbers, drivers' licence, work pass etc.) and copies of documents containing such national identification numbers; and

(ii) retention of physical documents containing national identification numbers (e.g. NRICs, passports, drivers' licence, work pass etc.).

For further details on the steps/processes to be followed/taken by Staff and Students in relation to their collection of national identification numbers/documents, please refer to Appendix 3.

2.3 Residential Address

A residential address, on its own, relates to a particular place and there could be several individuals residing there. Hence, whether a residential address constitutes personal data would depend on whether the address is associated with a particular identifiable individual so as to form part of the individual's personal data.

2.4 Biometric information

In the event the Personal Data involved falls within the definition of "Individually Identifiable" data (as defined in the Human Biomedical Research Act ("**HBRA**") 2015)), Staff and Students must, in addition to the obligations under the PDPA, also adhere to the obligations relating to the protection of such data as prescribed by the HBRA.

2.5 Research Data

Where the Personal Data involved falls within the definition of "Research Data" as defined in the NUS Research Data Policy Documents, Staff and Students must, in addition to the obligations under the PDPA, also adhere to the obligations relating to the protection of such Research Data as set out in the Research Data Policy Documents.

## 3 EXCLUDED PERSONAL DATA:

The PDPA does not apply to, or applies to a limited extent to, certain categories of Personal Data. For further details of such excluded Personal Data, please see Appendix 15 below.

## APPENDIX 3 - NATIONAL IDENTIFICATION NUMBERS & DOCUMENTS

### Legal Obligation

**1 STAFF/STUDENTS ARE GENERALLY NOT ALLOWED TO:**

(i) collect, use and disclose national identification numbers (e.g. NRIC numbers, passport numbers, drivers' licence, work pass etc.) and copies of documents containing such national identification numbers; and

(ii) retain physical documents containing national identification numbers (e.g. NRICs, passports, drivers' licence, work pass etc.).

1.1 Collection, use or disclosure of national identification numbers

Collection, use or disclosure of national identification numbers (or copies of documents containing such national identification numbers) may only be done under the following specified circumstances:

(i) Collection, use or disclosure of the national identification numbers (or copies of documents containing such national identification numbers) is required under the law (or an exception under the PDPA applies); or

(ii) Collection, use or disclosure of the national identification numbers (or copies of documents containing such national identification numbers) is necessary to accurately establish or verify the identities of the individuals to a high degree of fidelity.

1.2 Retention of physical documents containing national identification numbers

Staff/Students should not retain physical documents containing national identification numbers unless retention is required by law.

1.3 PDPC Guidelines

For further details and examples of when and how Staff/Students can collect, use, disclose and/retain national identification numbers/documents, please refer to the PDPC "Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers" (as the same may be amended/revised, updated and/or supplemented from time to time).

### Application & Implementation

**2 REQUIRED UNDER THE LAW (OR AN EXCEPTION UNDER THE PDPA APPLIES)**

2.1 Staff/Students may collect, use or disclose an individual's NRIC number (or copy of NRIC) without his or her consent if it is required under the law.

2.2 As good practice though, Staff/Students should still notify the individual of the purpose for the collection, use or disclosure, as the case may be.

**3 NECESSARY TO ACCURATELY ESTABLISH OR VERIFY THE IDENTITY OF THE INDIVIDUAL TO A HIGH DEGREE OF FIDELITY**

3.1 Where an organisation finds it necessary to accurately establish or verify the identity of the individual to a high degree of fidelity, it may collect, use or disclose his or her NRIC number with notification and consent.

3.2 Examples of situations that would be considered necessary to accurately establish or verify the identity of the individual to a high degree of fidelity:

(i) Where the failure to accurately identify the individual to a high degree of fidelity may pose a significant safety or security risk.

(ii) Where the inability to accurately identify an individual to a high degree of fidelity may pose a risk of significant impact or harm to an individual and/or the organisation (e.g. fraudulent claims).

## 4 ALTERNATIVES TO NRIC

For further details of alternative identifiers that Staff/Students can adopt instead of national identification numbers, please refer to the PDPC "Technical Guide to Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers" (as the same may be amended/revised, updated and/or supplemented from time to time.

## APPENDIX 4 - CONSENT OBLIGATION

### Legal Obligation

**1 STAFF/STUDENTS MUST:**

(i) only collect, use or disclose Personal Data for purposes which an individual has given his consent;

(ii) allow the individual to withdraw consent; and

(iii) upon withdrawal of consent, cease such collection, use or disclosure.

### Application & Implementation

**2 MUST BE OBTAINED PRIOR TO COLLECTION, USE OR DISCLOSURE**

Staff/Students must obtain the consent of an individual for the collection, use or disclosure of his/her Personal Data for any purpose, and such consent must be obtained on or before such collection, use or disclosure.

**3 CAN BE EXPRESS OR DEEMED CONSENT**

3.1 Express Consent

(i) Express consent is where the individual actively communicates his/her consent.

(ii) This can be communicated:

(a) in writing; or

(b) verbally.

3.2 Deemed Consent

(i) Deemed consent is where an individual does not actively indicate his/her consent but voluntarily provides his/her Personal Data for a purpose and it is reasonable that he/she would voluntarily provide his data.

(ii) Deemed consent will not cover purposes outside those for which the Personal Data was provided.

(iii) Types of Deemed Consent:

(a) Deemed consent by conduct

(b) Deemed consent by contractual necessity

(c) Deemed consent by notification

3.3 Deemed consent by conduct

(i) Deemed consent by conduct applies to situations where the individual voluntarily provides his Personal Data to the University. The purposes are limited to those that are objectively obvious and reasonably appropriate from the surrounding circumstances.

(ii) An individual may be regarded as voluntarily providing Personal Data where the individual takes certain actions that allow the data to be collected, without providing the data himself.

3.4 Deemed consent by contractual necessity

(i) The University can collect, use and disclose Personal Data where it is reasonably necessary to fulfil the contract with the individual.

(ii) An individual is deemed to consent to the following where reasonably necessary for the conclusion of the contract/transaction between the individual and NUS:

(a) the disclosure of that Personal Data by NUS to another organisation;

(b) the collection and use of that Personal Data by the other organisation; and

(c) the subsequent disclosure of that Personal Data by the other organisation in question to further organisations.

3.5 Deemed Consent by Notification:

(i) An individual may be deemed to have consented to the collection, use or disclosure of his Personal Data by the University for a purpose he has been notified of if he has not taken any action to opt out of this

Before collection, using or disclosing any Personal Data about the Individual, the Staff/Student must do the following:

(a) Conduct an assessment;

(b) Provide adequate notification; and

(c) Provide a reasonable opt-out period.

(ii) Conduct an assessment:

Staff/Students must:

(a) conduct an assessment to determine that the proposed collection, use or disclosure of the Personal Data is not likely to have an adverse effect on the individual;

(b) identify any adverse effect that the proposed collection, use or disclosure is likely to have on the individual, and consider and implement reasonable measures to eliminate, reduce the likelihood of or mitigate the adverse effects identified. For further details on conducting the assessment, please refer to the PDPC "Assessment Checklist for Deemed Consent by Notification" and "Advisory Guidelines on key concepts in the PDPA" as well as the Personal Data Protection Regulations 2021 (as the same may be amended/revised, updated and/or supplemented from time to time);

(iii) Provide adequate notification:

Staff/Students must take reasonable steps to bring the following information to the attention of the individual:

(a) the University's intention to collect, use or disclose the Personal Data;

(b) the purpose for which the Personal Data will be collected, used or disclosed;

(c) a reasonable period within which, and a reasonable manner by which, the individual may notify the University that the individual does not consent to NUS' proposed collection, use or disclosure of the Personal Data;

(iv) Provide a reasonable opt-out period:

(a) Staff/Students must provide a reasonable period for the individual to opt out before it proceeds to collect, use or disclose the Personal Data.

(b) Any collection, use or disclosure of Personal Data for the purposes that have been notified should commence only after the expiry of the opt-out period.

## 4 CONSENT MUST BE RECORDED

4.1 Staff/Students must record all consent obtained in a manner that is accessible for future reference.

4.2 Written Consent:

(i) As a matter of best practice, Staff/Students should try to obtain consent in written form.

Example:

(ii) Where an individual completes and signs off on a consent form, or where the individual ticks a box on a form stating that he consents to the collection, use or disclosure of his Personal Data, this consent would be express.

4.3 Verbal Consent:

(i) If written consent is not possible and only verbal consent is available, Staff/Students must record such consent in a manner that is accessible for future reference.

Example:

(ii) A written note can be taken down and the individual be made to sign on the note.

(iii) An email or letter (assuming that the verbal consent provided extends to allowing such an email or letter to be sent) can be sent to the individual to note that his verbal consent was obtained on a specified date.

## 5 COLLECTING PERSONAL DATA FROM A PERSON ACTING ON BEHALF OF ANOTHER INDIVIDUAL

When collecting Personal Data from a person ("X") acting on behalf of another individual ("Y"), Staff/Students must:

(i) check with "Y" that he/she has given consent for such collection; or

(ii) ensure that consent is given by any person validly acting on behalf of "Y" for the collection, use or disclosure of such Personal Data.

## 6 RECEIVING PERSONAL DATA FROM THIRD PARTIES

6.1 When Personal Data of an individual is obtained from third parties, there is a risk that such third parties had failed to collect the Personal Data in compliance with the PDPA (e.g. the third party may have failed to obtain the necessary consent from the individual at the time the third party had collected the individual's Personal Data).

6.2 Without the individual himself/herself voluntarily providing the Staff/Student with his/her Personal Data, the Staff/Student cannot know that that individual has authorised a third party

to provide the Staff/Student with his/her Personal Data unless the third party can show evidence that the individual has consented to this.

6.3 Wherever possible, whenever Staff/Students collect the Personal Data of an individual from a third party, they should notify and obtain the consent of the individual directly.

6.4 Staff/Students can only collect and receive Personal Data of individuals from third parties if:

(i) there is a legitimate business purpose for the Staff/Student or their department/unit to receive Personal Data of individuals from third party organisations or third party individuals; and

(ii) the Staff/Student has cleared such arrangement with the Data Protection Office prior to collecting such Personal Data.

6.5 Where Personal Data of an individual is collected from a third party and it is not reasonably practicable for the University to notify and obtain the consent of the individual directly, the Staff/Student must not allow the Personal Data to be collected unless:

(i) there is a legitimate business purpose for the Staff/Student or their department/unit to receive Personal Data of individuals from third party organisations or third-party individuals; and

(ii) he/she is *satisfied that the third party providing the Personal Data of individuals has obtained the consent of those individuals to disclose their Personal Data to the University for the specified purpose(s)

*For the purposes of verifying whether a third-party source can validly give consent or has obtained consent from the individual concerned, the relevant Data Steward may employ one or more of the following means (as applicable in the particular context):

(i) Ensure that contractual warranties and/or obligations requiring the third party to obtain the individual's consent prior to disclosing Personal Data to the University and requiring the third parties to warrant that they have the authority/consent from the individual to provide the individual's Personal Data to the University has already been included in the contract with such third party;

(ii) Seek an undertaking from the third party through a term of contract between NUS and the third party that the disclosure to NUS for NUS's purposes is within the scope of the consent given by the individual to the third party;

(iii) Obtain confirmation in writing from the third party;

(iv) Obtain, and document in an appropriate form, verbal confirmation from the third party; and/or

(v) Obtain a copy of the document(s) containing or evidencing the consent given by the individuals' concerned to the third party to disclose the Personal Data.

6.6 If the Staff/Student is unable to satisfy the conditions listed above, the Staff/Student must not allow the Personal Data to be collected from the third-party individual unless the Staff/Student has cleared such arrangement with the Data Protection Office prior to collecting such Personal Data.

## 7 MUST BE OBTAINED LAWFULLY

Staff/Students must:

(i) collect Personal Data using lawful and fair methods, without deception, intimidation or unreasonable intrusiveness

(ii) ensure that they do not obtain consent by providing false or misleading information or through deceptive or misleading practices.

## 8 MUST NOT BE A CONDITION TO PROVIDING A PRODUCT OR SERVICE

Staff/Students cannot require an individual to consent to the collection, use or disclosure of his/her Personal Data as a condition of providing a product or service where such collection, use or disclosure of the Personal Data is beyond what is reasonable to provide the product or service to that individual.

## 9 MUST RELATE TO SPECIFIC PURPOSE

Staff/Students must ensure that the specific purpose(s) for which they will be collecting, using or disclosing the Personal Data are captured when seeking an individuals' consent at the point of collection/use/disclosure of his/her Personal Data.

## 10 FRESH CONSENT REQUIRED FOR DIFFERENT PURPOSE

10.1 The use and disclosure of any Personal Data collected must be consistent with the original purpose it was intended for.

10.2 Staff/Students must obtain fresh consent from the individual again before the Personal Data is used for another purpose (i.e. different the original purpose).

(i) Example 1:

Where consent has been previously obtained from an individual for the collection, use or disclosure of his Personal Data for purposes A, B and C, and the Staff/Student now want to use the individual's Personal Data for other purposes (e.g. purposes D and E), fresh consent must be sought from the individual to use or disclose his Personal Data for such other purposes before the Staff/Student processes that individual's Personal Data for such other purposes.

Example 2:

There may be occasions where corporate partners of NUS wish to insert their marketing and/or informational brochures into the letters NUS intends to send to individuals (whether students, staff or otherwise). As NUS may not have obtained the requisite consent from the individuals to send such individuals marketing and/or information brochures of NUS' corporate partners, Staff/Students **should not include any marketing and/or informational brochures of NUS' corporate partners in any of NUS' letters to individuals, unless the prior written approval of DPO has been obtained.**

(ii) If Staff/Students are unclear whether a certain use or disclosure falls within the scope of the original consent provided, they should seek clarification and assistance from the Data Protection Office.

## 11 CONSENT CAN BE WITHDRAWN

11.1 Under the PDPA, individuals have the right to withdraw his/her consent fully or partially for the collection, use and/or disclosure of Personal Data in the possession or control of NUS, unless there are reasonable business or legal grounds for refusal to comply with such request.

11.2 Upon receipt of any notice of a withdrawal of consent from any individual, Staff/Students shall:

(i) not prohibit any individual from withdrawing consent (although this does not affect any legal consequences arising from such withdrawal);

(ii) inform the individual of the consequences of their withdrawal of consent and the time required for processing such withdrawal;

(iii) direct the individual to put up a request for such withdrawal through the through the central Personal Data service request system ("**PSR**"), a link to which is publicly available on the NUS website; and

(iv) cease (and cause any data intermediaries and agents to cease) collecting, using or disclosing the Personal Data.

11.3 Data Protection Office Assessment:

(i) Via the PSR system, the request will automatically be received by the Data Protection Office.

(ii) The Data Protection Office will assess based on the type of request which departments to involve and will send out a report to the PDPA POCs containing information regarding the request and ask the PDPA POCs to fill in a form and send it back as soon as possible.

(iii) As there are statutory time limits to comply with, when responding to these types of request, Staff/Students involved in such requests either via the Data Protection Office or via the PDPA POCs must assist within the given timeframe.

(iv) Where it is decided to comply with a request, it is important upon instruction of the Data Protection Office to process the withdrawal of consent and thereafter cease collecting, using and/or disclosing the individual's Personal Data as per the manner stated in the request.

(v) If the Data Protection Office is satisfied on reasonable grounds that a request should not be complied with, NUS need not comply with the withdraw of consent. If the individual's correction request is not acceded to, it is good practice to record down the date on which a request was sought and the reasons for not acceding to the request.

## APPENDIX 5 - PURPOSE LIMITATION OBLIGATION

### Legal Obligation

**1 STAFF/STUDENTS:**

(i) can only collect, use or disclose Personal Data about an individual for the purposes for which the individual has given consent; and

(ii) must limit their collection, use or disclosure of the individual's Personal Data only to such purposes.

### Application & Implementation

**2 PURPOSE MUST BE REASONABLE AND NECESSARY**

2.1 Staff/Students must only collect, use or disclose Personal Data for purposes:

(i) that a reasonable person would consider appropriate in the circumstances;

(ii) that are necessary for their functions/activities.

2.2 Staff/Students must not request consent to process more Personal Data than they need to fulfil their purpose. (E.g. Indicate on data collection forms which fields are optional and compulsory.)

**3 SUFFICIENTLY DETAILED**

Purposes notified to the individuals must be sufficiently detailed.

**4 PURPOSE REVIEWED BY INDIVIDUAL**

Staff/Students should ensure that the individuals have indeed have reviewed the purposes before providing their consent.

**5 DATA PROTECTION OFFICE GUIDANCE**

Where it is unclear whether any purpose is reasonable, seek clarification from Data Protection Office.

## APPENDIX 6 - NOTIFICATION OBLIGATION

### Legal Obligation

### 1 DATA SUBJECT MUST BE NOTIFIED OF PURPOSE PRIOR TO COLLECTION, USE OR DISCLOSURE

Staff/Students must notify an individual of the purposes for which they are intending to collect, use or disclose his/her Personal Data on or before the collection, use or disclosure of Personal Data.

### Application & Implementation

### 2 ADEQUATE MEASURES & PROTECTION

2.1 Staff/Students must take adequate measures to protect personal data which they disclose to third parties by putting in place contracts containing adequate PDPA clauses and indemnities. Staff/Students must also ensure that their agreements, procurement contracts, service contracts, non-disclosure agreements or any other documents/contracts contain adequate PDPA clauses.

2.2 Staff/Students must seek guidance from DPO (in consultation with OLA as required) if they have any queries or concerns, including, but not limited to, if they are unsure as to:

(i) Whether PDPA clauses are required ;

(ii) What PDPA clauses to use;

(iii) The application of any data protection principles; and/or

(iv) The appropriate methods of compliance.

### 3 NOTIFICATION CHANNELS

3.1 Personal Data collected on a form – State the purpose on the form.

3.2 Personal Data collected using a HTTP cookie, web beacons or other like methods – State the purpose on the website.

3.3 Personal Data collected over the phone – Notify individuals of the purpose using recorded messages (where feasible)

## APPENDIX 7 - ACCURACY OBLIGATION

### Legal Obligation

**1 STAFF/STUDENTS MUST**

Take reasonable efforts to ensure that Personal Data collected by or on their behalf is accurate and complete, if it is likely to be used to make a decision that affects the individual, or if it is likely to be disclosed to another organisation.

### Application & Implementation

**2 ENSURE PERSONAL DATA COLLECTED IS REASONABLY ACCURATE AND COMPLETE**

2.1 When:

Staff/Students must take reasonable effort to ensure that the Personal Data collected is accurate and complete if:

(i) the Personal Data is likely to be used by NUS to make a decision that affects the individual to whom the Personal Data relates, or

(ii) the Personal Data is likely to be disclosed to another organisation.

2.2 How:

To ensure that the Personal Data collected is accurate and complete, Staff/Students must:

(i) accurately document all Personal Data they collect (whether directly from the individual concerned or through another organisation);

(ii) ensure that the Personal Data collected includes all relevant parts (i.e. complete);

(iii) verify Personal Data collected against supporting documents;

(iv) only grant access to Personal Data to authorised Staff/Student on a strictly need-to-know basis in order to minimise the risk of compromising data integrity;

(v) consider whether there is any doubt as to the accuracy of any Personal Data that has been provided directly by a particular individual and if so, require that particular individual to undertake that the Personal Data they have provided is accurate;

(vi) where it is crucial whether the Personal Data is up-to-date, take steps to verify that the Personal Data provided by the individual is current; and

(vii) where Personal Data is collected from a third-party source, obtain confirmation from the source that accuracy and completeness of the Personal Data has been verified.

**3 REQUIREMENT OF "REASONABLE EFFORTS"**

3.1 The amount of effort required of a Staff/Student in ensuring the accuracy and completeness of the Personal Data collected depends on the circumstances at hand and factors to be considered include (but are not limited to):

(i) the nature of the Personal Data and its significance to the individual (i.e. the more 'sensitive' the information, the more efforts would need to be undertaken to ensure its accuracy and correctness);

(ii) the purpose for which the Personal Data is collected, used or disclosed (i.e. the more the purpose affects the individual concerned, the more efforts would need to be undertaken to ensure its accuracy and correctness);

(iii) the reliability of the Personal Data (whether it was obtained from a reliable source or through reliable means);

(iv) the currency of the Personal Data (whether the data is recent or was first collected some time ago); and

(v) the impact on the individual concerned if the Personal Data is inaccurate or incomplete.

3.2 The accuracy principle does not necessarily require Staff/Students to check the accuracy and completeness of an individual's Personal Data each and every time they use such Personal Data of the individual. It depends on the circumstances and factors such as the above. If in doubt, Staff/Students should consult their respective PDPA POCs.

## APPENDIX 8 - PROTECTION OBLIGATION

### Legal Obligation

### 1 STAFF/STUDENTS MUST

Take reasonable security measures to protect the Personal Data of individuals that is in their possession or control, in order to prevent unauthorised access, use, disclosure or similar risks.

### Application & Implementation

### 2 REQUIREMENTS UNDER THE NUS POLICY DOCUMENTS

Staff/Students must protect all Personal Data that they or NUS process in the course of their daily operational activities for NUS and/or in the course of their employment). In particular, Staff/Students must adhere to the requirements, obligations and standards relating to the storage, protection, use and disclosure of Personal Data set out in:

(i) this Policy Document;

(ii) the NUS IT Policy Documents; and

(iii) all other NUS internal documents/directions regarding the security of data, use of data etc.

### 3 ADDITIONAL SECURITY MEASURES

3.1 In addition, and without derogating from the provisions and requirements set out in the NUS IT Policy Documents, Staff/Students must also assess and implement such security measures as they consider reasonable and appropriate, taking into consideration factors such as (but not limited to):

(i) the nature of the Personal Data in question

(ii) the form the Personal Data takes (i.e. physical or electronic medium)

(iii) the impact level and potential harm of any loss/leak/modification of the data in question

(iv) whether the Personal Data will be shared with third parties or third parties will otherwise have access to the Personal Data

3.2 Examples of Security Measures

Some security measures that Staff/Students should consider adopting are set out in the paragraphs below. Please note that the measures listed below are not meant to be exhaustive and Staff/Students must determine the most appropriate measures to adopt given their specific circumstances.

(i) Administrative Measures:

(a) Grant access to Personal Data to authorised Staff/Student on a strictly need-to-know basis.

(b) Only hold on the appropriate amount of Personal Data to reduce the efforts required to protect Personal Data.

(ii) Physical Measures:

(a) Clearly and conspicuously mark/identify documents containing Personal Data.

(b) Store and archive documents after use.

(c) Store any documents containing Personal Data in secure locations (e.g. locked cupboards)

(d) Install access control systems (e.g. key card/biometric door access).

(e) Employ security alarm systems to detect access by unauthorised parties.

(f) Track movement of documents containing Personal Data, particularly where such documents are being moved between different offices.

(g) Adopt clean desk practices.

(h) Use privacy filters to prevent unwanted/unintended/unauthorized viewers from viewing on-screen information.

(i) Dispose of documents containing Personal Data that are no longer required in an appropriate manner (e.g. shred, incinerate).

(iii) When delivering/transferring physical data, implement and adhere to such measures and means of delivery as are necessary to provide the appropriate level of protection, including, but not limited to:

(a) Place documents containing Personal Data in envelopes that are:

i. accompanied by a list of the items contained in the envelope;

ii. clearly and sufficiently marked with the name/location of the recipient;

iii. sealed with tamper evident stickers and marked "Confidential – To be opened by Addressee only"; and

iv. sufficiently secure for the documents in question (e.g. it should not be possible to peruse the contents of the document through the envelope).

(b) Pass documents securely to the intended recipient, with direct interface between the deliverer and recipient where possible/appropriate (e.g. Where the recipient is not at his/her desk/office, the document must be redelivered at a subsequent time or a note can be left for the recipient to collect the document etc.).

(c) If a courier is required, only use a reliable courier service with procedures for registration, on-route tracking and acknowledgement of receipt by the intended recipient.

(d) Technical Measures*

i. Verify that IT service providers are able to provide the degree of IT security required.

ii. Install suitable cybersecurity software (including email- screening, antivirus, firewall etc.) and use appropriate computer security settings.

iii. Implement suitable access controls (e.g. 2 factor authentication, user passwords, screen saver passwords, restricting access to shared network drives only to authorised persons).

*Note: If in doubt, please consult NUS IT.

(iv) Communication Security Measures

(a) Destination Information:

Check and ensure destination information (e.g. mailing address, email address and facsimile number) is correct and matches that of the intended recipient before sending out communications containing Personal Data.

(b) Identity of Recipient:

Check and verify the identity of the recipient(s) before giving out Personal Data via the telephone or other means.

(c) In-transit protection

Where technically possible and/or operationally feasible, encrypt and/or password protect all emails/documents containing Personal Data.

| **Internal Emails** | **External Emails** | **All attachments** |
|---|---|---|
| Use encryption option(s) available in Microsoft Office | <u>Option 1:</u><br><br>No Personal Data to be included within the body of an external email.<br><br>Move any Personal Data into a password-protected document as an attachment.<br><br>Communicate password to the recipient via a mechanism other than email (e.g. Skype for Biz, SMS, WhatsApp etc).<br><br><u>Option 2:</u><br><br>If Personal Data is included in the body of the email, then the information should be masked (e.g. Masking IC numbers by using only using last 3 digits + last alphabet) | Password protect all attachments with Personal Data content.<br><br>Communicate password to the recipient via a mechanism other than email. |

(v) Additional Options

Please refer to the NUS Data Management Policy 3.0 Appendices – Appendix G: Data Protection.

## APPENDIX 9 - RETENTION LIMITATION OBLIGATION

### Legal Obligation

**1 STAFF/STUDENTS MUST**

Cease retention or remove the means by which the Personal Data can be associated with particular individuals when:

(i) it is reasonable to assume that the purpose for initially collecting the Personal Data is no longer required; and

(ii) there is no legal or business purpose for retaining the Personal Data.

### Application & Implementation

**2 RETENTION PERIODS**

2.1 The PDPA does not specify any specific duration of time for which an organisation may legitimately retain Personal Data or any category of Personal Data.

2.2 Staff/Students must adhere to the retention requirements and periods set out in:

(i) NUS's Retention Policy for Personal Data of Staff;

(ii) NUS's Policy on Retention and Archival of Student Academic and Curriculum record;

(iii) the NUS IT Policy Documents;

(iv) Individual retention policies for Personal Data set, managed and administered Data Stewards of centralised functional areas (e.g., Registrar's Office, Office of Finance, Office of Human Resources, Development Office, Office of Alumni Relations, etc.) and the respective Departments, units, schools and faculties across NUS community; and

(v) any other applicable policies/guidelines/procedures relating to the retention and archival of University Data, as may be issued and/or amended from time to time by NUS.

(vi) Staff/Students who are unsure if a retention policy exists for their department/unit etc. and/or what the appropriate approach would be in case no specific retention policy exists should consult their PDPA POCs.

**3 WHAT CONSTITUTES "CEASING RETENTION"**

An organisation ceases to retain documents containing Personal Data when it, its agents and its data intermediaries no longer have access to those documents and the Personal Data they contain.

**4 EXAMPLES OF "CEASING RETENTION"**

Staff/Students may cease to retain Personal Data by employing any of the following means as appropriate:

(i) Return all documents containing an individual's Personal Data to the individual in question (or such other person as the individual may direct) without keeping any copies (whether electronic or non-electronic)

(a) Ensure the return is clearly documented and duly acknowledged by the individual

(ii) Destroy/dispose of the documents containing an individual's Personal Data

(a) The means of destruction/disposal employed must be appropriate for the form of the Personal Data (e.g. physical or electronic)

(b) Staff/Students must adhere to the destruction/disposal requirements prescribed in the NUS IT Policy Documents.

(c) If Staff/Students are of the view that the destruction/disposal methods prescribed in the NUS IT Policy Documents are not adequate or appropriate for the circumstances and Personal Data in question, they must seek further guidance from NUS IT on the appropriate means to employ.

## 5 EXAMPLE OF "REMOVING THE MEANS BY WHICH THE PERSONAL DATA CAN BE ASSOCIATED WITH PARTICULAR INDIVIDUALS" – ANONYMISATION

5.1 Definition

Anonymising the individual's Personal Data refers to the process of removing identifying information, such that the remaining data does not identify any particular individual, whether directly by itself, or indirectly in conjunction with any other data or information to which the University has or is likely to have access.

5.2 When to Consider Anonymisation?

5.2.1 Data Stewards may wish to consider anonymisation as a means of complying with the obligation to cease to retain Personal Data once it is no longer necessary for any legal or business purpose if the anonymised data can still be valuable and/or of use to the University.

5.2.2 Several techniques exist for anonymization. For further information on the different techniques, please access the PDPC website and refer to the PDPC's "Guide to Basic Data Anonymization Techniques" and/or such other guidelines as may be issued and/or amended by the PDPC from time to time.

5.3 Re-identification

5.3.1 Data Stewards should be mindful of the possibility that anonymised data can in certain circumstances, be re-identified and constitute Personal Data again.

5.3.2 Data Stewards should be particularly mindful of such risks if the University intends to publish or disclose Personal Data that has been anonymised.

## APPENDIX 10 - TRANSFER LIMITATION OBLIGATION

### Legal Obligation

**1 STAFF/STUDENTS MUST ONLY TRANSFER PERSONAL DATA TO A COUNTRY OUTSIDE SINGAPORE IN ACCORDANCE WITH THE REQUIREMENTS PRESCRIBED UNDER THE PDPA, NAMELY:**

(i) take appropriate steps to ensure that NUS will continue to comply with the PDPA in respect of the transferred Personal Data while it remains in the possession or under the control of NUS; and

(ii) take appropriate steps to ascertain whether and ensure that the recipient of the Personal Data overseas is bound by legally enforceable obligations to provide to the Personal Data transferred a standard of protection that is comparable to that under the PDPA.

### Application & Implementation

**2 WHEN IS PERSONAL DATA TRANSFERRED OUT?**

2.1 Personal Data is transferred out when an individual's Personal Data leaves the territorial limits of Singapore.

2.2 For example, this could be by way of:

(i) Personal Data that is in the body of an email sent by you while you are in Singapore to an email recipient outside of Singapore;

(ii) Transferring Personal Data to a third party overseas for data storage, backup or disaster recovery purpose (the third party could include a sister company, an unaffiliated third party, a data centre);

(iii) Personal data in an email attachment sent to a recipient that is overseas.

**3 REQUIREMENTS FOR TRANSFERRING PERSONAL DATA OVERSEAS**

**Before Staff/Students can transfer Personal Data overseas, they must:**

| | **Requirement** | **How** |
|---|---|---|
| 3.1 | Take appropriate steps to ensure that NUS will continue to comply with PDPA requirements while the Personal Data remains in NUS' possession or control | Whilst the Personal Data remains in the Staff/Student's control, they must adhere to the requirements set out in:<br>(i) the NUS IT Policy Documents;<br>(ii) this Personal Data Protection Policy & Procedures;<br>(iii) the Research Data Policy Documents (if applicable); and<br>(iv) any other NUS Policy Documents relating to the management and treatment of University Data (including such additional Policy Documents as the University may from time to time issue). |
| 3.2 | Ensure that the overseas organization provides a standard of protection comparable to that under the PDPA for the Personal Data | **Consult Office of Legal Affairs**<br><br>(i) Enter into a written contract with the overseas organization approved by OLA. |

| | | |
|---|---|---|
| | transferred | (ii) Verbal consent or declaration by the data intermediary is not sufficient or acceptable.<br>(iii) Where a third party refuses to do so, you must not provide them with the Personal Data.<br>(iv) Consult OLA for the standard clauses and templates to be used in the various contracts/agreements to ensure that the contract with the overseas organisation has adequate language and provisions to:<br>(a) ensure NUS' compliance with the PDPA Legislation;<br>(b) limit NUS' liability under the PDPA Legislation; and<br>(c) protect NUS against claims for any breach of the PDPA which had been caused by the third party. |
| | | **Consult Data Protection Office**<br><br>Data Protection Office to assess:<br><br>(i) if NUS should obtain consent; or<br>(ii) can rely on any of the exceptions provided for in the PDPA.<br><br>(1) <u>Clear informed consent</u>:<br><br>In order to rely on consent:<br><br>(i) the individual must be provided with a reasonable summary in writing of the extent to which the Personal Data to be transferred will be protected to a standard comparable to the protection under the PDPA<br>(ii) the consent must not be a condition of providing a product or service, (unless the transfer is reasonably necessary); and<br>(iii) the Consent must not have been obtained by the provision of false or misleading information or other deceptive practices.<br><br>(2) <u>Exceptions</u>:<br><br>(i) The transfer is necessary for the performance of a contract between NUS and the individual; or<br>(ii) The transfer is necessary for the conclusion or performance of a contract between NUS and a third party which is entered into at the individual's request, or which a reasonable person would consider to be in the individual's interest. |
| | | **Consult NUS IT** |

| | | |
|---|---|---|
| | | Staff/Students must consult NUS IT and ensure compliance with the NUS IT Policy Documents (including, but not limited to, the NUS Cloud Policy). |

## APPENDIX 11 - ACCESS & CORRECTION OBLIGATION

### Legal Obligation

**1 STAFF/STUDENTS MUST, UPON REQUEST:**

(i) provide an individual with the Personal Data and information about the ways in which his/her Personal Data has been or may have been used or disclosed within 1 year before the request; and

(ii) correct any error or omission in an individual's Personal Data and send the corrected data to other organisations to which the Personal Data was disclosed by NUS within 1 year before the correction is made.

### Application & Implementation

**2 REQUEST**

Upon receipt of any notice to access/correct Personal Data from any individual, Staff/Students must:

(i) verify the identity of the individual or entity requesting access to or correcting Personal Data;

(ii) if the access/correction request is being made on behalf of another person, obtain evidence of consent from the person to whom the Personal Data belongs;

(iii) if the access request is in respect of a deceased individual who has been dead for 10 years or less, ensure that the access is only being provided to authorised person(s) acting on behalf of the deceased person's estate; and

(iv) direct the individual to put up a request for such access/correction through the central PSR.

**3 DATA PROTECTION OFFICE ASSESSMENT**

3.1 Via the PSR system, the request will be received by the Data Protection Office automatically.

3.2 The Data Protection Office will assess based on the type of request which departments to involve and will send out a report to the PDPA POCs containing information regarding the request and ask the PDPA POCs to fill in a form and send it back as soon as possible.

3.3 As there are statutory time limits to comply with, when responding to these types of request, Staff/Students involved in such requests either via Data Protection Office or via the PDPA POCs must assist within the given timeframe.

3.4 When processing requests for access, Staff/Students must:

(i) grant access to the Personal Data and provide information about the use and disclosure of such data within a year before the date of the request, as soon as reasonably possible and in any event, no later than 30 days after receiving the request. If the Staff/Student is unable to respond to an access request within 30 days after receiving the request, the Staff/Student shall inform the individual in writing within 30 days of the time by which it will be able to respond to the request;

(ii) consider whether to charge any costs for providing access (e.g. for disbursements such as photocopying or postal fees), and to inform the requestor of such costs accordingly;

(iii) provide the requestor with only the requested information.

3.5 When processing requests for correction, the Staff/Student must:

(i) make the necessary correction(s) as soon as practicable from the time the correction request is made and in any event, no later than 30 days from the time the request is made. If the Staff/Student is unable to respond to an access request within 30 days from the time the request is made, the Staff/Student shall inform the individual in writing within 30 days of the time by which it will be able to correct the Personal Data;

(ii) send the corrected Personal Data to every other organisation to which the Personal Data was disclosed by NUS within a year before the date the correction was made, unless that other organisation does not need the corrected Personal Data for any legal or business purpose; and

(iii) inform the individual upon completion of the correction request.

3.6 If the Data Protection Office is satisfied on reasonable grounds that a request should not be complied with, Staff/Students:

(i) need not give the requested access to Personal Data or make the requested correction;

(ii) may, if practicable, provide the individual with reasons for refusing the access/correction (e.g. falls under an exception provided for in the PDPA); and

(iii) must preserve a complete and accurate copy of the withheld Personal Data requested in the individual's access request ("withheld personal data") for a period of at least 30 calendar days after rejecting the access request – as the individual may seek a review of NUS' decision.

## APPENDIX 12 - DATA BREACH NOTIFICATION OBLIGATION

### 1 EXAMPLES OF DATA BREACH

1.1 Data Breaches may occur in a variety of circumstances, such as, but not limited to:

(i) Loss or theft of Personal Data, equipment on which Personal Data is stored (e.g. a memory stick) or paper records;

(ii) Inappropriate access controls allowing unauthorised use of Personal Data (e.g. uploading Personal Data to an unsecured web domain, using unsecure passwords);

(iii) Equipment failure where Personal Data stored in such equipment may be affected;

(iv) Personal Data left unlocked/unprotected in accessible areas (e.g. leaving IT equipment unattended when logged into a user account);

(v) Disclosing Personal Data to unauthorised individuals or an untrusted environment;

(vi) Collection of Personal Data by unauthorised individuals;

(vii) Human error/accidental disclosure of Personal Data (e.g. emails containing personal information sent to the wrong recipient);

(viii) Hacking, viruses or other security attacks on IT equipment systems or networks; and/or

(ix) Breaches of physical security (e.g. forcing of doors/windows/filing cabinets) where the intruder may gain access to Personal Data.

1.2 If there is any doubt as to whether a Data Breach has occurred, Staff/Students should consult the Data Protection Office immediately.

### 2 REPORT ACTUAL/POTENTIAL DATA BREACHES TO THE DATA PROTECTION OFFICE IMMEDIATELY

2.1 Staff/Students who are involved in or aware of any Data Breach must:

(i) immediately report any such Data Breaches or the possibility of such Data Breaches to the NUS Data Protection Office;

(ii) comply with any other applicable prevailing University procedures for incidents of Data Breach, including but not limited to the NUS IT Policy Documents and any procedures derived therefrom; and

(iii) comply with any directions as may be prescribed by the Data Protection Office and/or NUS IT.

2.2 Delay in or failure to report

2.2.1 Staff/Students should report any breach immediately as speed of reporting is important.

2.2.2 Staff/Students who are aware that their action or omission has caused a breach and yet fail delay or fail to report such breach will be subject to more severe consequences than if they report the breach immediately.

## APPENDIX 13 - ACCOUNTABILITY OBLIGATION

### Legal Obligation

**1 STAFF/STUDENTS MUST:**

(i) adhere to the data obligations under the PDPA and NUS' data protection policies and procedures; and

(ii) act on feedback from our various stakeholders.

### Application & Implementation

**2 STAFF/STUDENTS MUST:**

(i) be familiar with and know the location of NUS' data protection policies and the related practices/procedures and processes, including but not limited to the complaints process and measures to be taken when handling complaints received; and

(ii) be aware of the identity and business contact information of NUS' DPO and whom to direct queries to regarding Personal Data protection.

## APPENDIX 14 - DO NOT CALL POLICY & PROCEDURES

### 1 RATIONALE & OBJECTIVES

1.1 The PDPC has established a Do Not Call ("**DNC**") regime/framework to enable individuals to register their Singapore telephone number(s) with the national DNC registry if they do not wish to receive marketing messages through their Singapore telephone number. The DNC regime/framework came into force on 2 January 2014 and the national DNC registry is operated by the PDPC.

1.2 All Staff and Students must strictly comply with the obligations under the DNC regime and are expected to be fully aware of the do's and don'ts relating to telemarketing, the sending of marketing SMSes/MMSes, marketing faxes and the making of marketing voice calls.

1.3 Should NUS be fined for breaches of the DNC regime/framework as a result of an action or omission of any Staff or Student, NUS reserves its right to claim compensation and damages from that Staff or Student.

### 2 SCOPE

2.1 Mode Of Message

The DNC regime/framework will only apply to Marketing Messages sent to a Singapore telephone number over three modes: voice calls, text messages or fax messages. For the avoidance of doubt, the DNC regime/framework will also cover Marketing Messages sent via data applications which use a Singapore telephone number, for example, Whatsapp, iMessage, Viber, etc.

2.2 DNC Registers

The PDPC maintains three registers for each mode of message. Since 2 December 2013, individuals may register their Singapore telephone numbers on any of these registers.

2.3 Marketing Message

(i) The DNC regime/framework will only apply to messages of a marketing nature ("**Marketing Messages**"), which is generally a message where the purpose, or one of the purposes, of the message, is to advertise or promote goods or services.

(ii) For example, the following messages will be considered Marketing Messages:

(a) messages promoting Alumni events that promote the sale of goods or services by NUS and/or NUS' partners

(b) messages seeking new enrolment or admissions into NUS or faculties

(c) messages selling items where part of the proceeds go to a charity or fund-raising cause

(d) messages promoting joint events between NUS and other partners where goods and services are advertised or promoted

(e) messages advertising or promoting goods or services of external companies that have sponsored a NUS event

(f) messages promoting an investment opportunity in a technology start up that is collaborating with NUS' research departments and/or faculties

2.4 Messages NOT impacted by the DNC regime/framework

2.4.1 The DNC regime/framework does not apply to messages that do not fall within the above scope i.e. a message where the purpose, or one of the purposes, is ***not*** to advertise or promote goods or services. For example, a message sent ***solely*** to solicit donations for a charitable cause by the Development Office.

2.4.2 As with the general nature of exceptions, these are to be construed narrowly. When in doubt on whether an exception under the PDPA applies, contact the Data Protection Office.

---

## B. POLICY STATEMENTS

---

## 3 THE PROHIBITIONS/RESTRICTIONS

3.1 Under the PDPA, there are 3 key requirements or prohibitions that must be complied with prior to contacting an individual with a Marketing Message through voice call, text messages or fax messages.

3.1.1 **Requirement To Check With National DNC Registry** – Check with the relevant national DNC Register (voice, text or fax) prior to sending the Marketing Message. There is an exception to this requirement where the individual to be contacted has previously given his or her *clear and unambiguous consent in evidential form* to receive Marketing Messages via the respective mode of communication (voice, text or fax).

3.1.2 **Requirement To Provide Contact Information** – Ensure that the Marketing Message contains clear and accurate information that identifies the organization as well as provides the organization's contact details, and also that the information in the Marketing Message is valid for at least 30 days after the individual has received the message.

3.1.3 **Voice Calling Line Identity** – Ensure that if the Marketing Message is communicated over a voice call, that the calling line is not concealed.

## 4 STAFF/STUDENTS OBLIGATIONS

4.1 Following the above obligations of NUS under the PDPA, NUS has put in place policy and procedures to be adhered to by all Staff and Students before contacting any individual for any marketing purpose.

4.2 All Staff and Students are to follow NUS' DNC policy and procedures before contacting any individuals for any marketing purpose. When in doubt, contact the Data Protection Office.

4.3 Note that there is to be **STRICTLY NO SENDING OF MARKETING MESSAGES VIA PHONE CALLS, TEXT MESSAGES OR FAX** without the specific written authorisation from the Data Protection Office.

4.4 Any individual, department or office seeking to send any marketing message via phone calls, text messages or fax shall seek authorisation from the Data Protection Office by submitting the NUS Telemarketing Authorisation Request Form to the Data Protection Office as set out at Annex A, no less than five business days prior to the intended start date of the sending of the marketing message.

4.5 With effect from 2 January 2014, the individual, department or office shall not send any marketing message until it has received the specific written authorisation from the Data Protection Office. The Data Protection Office also reserves the right to request for further information as well as amendments to the form and mode of marketing and to impose other obligations/requirements on the sending of the marketing message, as may be deemed necessary by the Data Protection Office to ensure NUS' compliance with the PDPA.

4.6 When the written authorisation to send marketing messages has been given by the Data Protection Office, ensure that all marketing messages provide clear and accurate information that identifies NUS and its contact details, and that the information in the message is valid for at least 30 days after the recipient receives it. If the message is to be communicated over a phone call, ensure that the telephone number making the call is not concealed.

## 5 NUS DNC REGISTRY

NUS has established an internal NUS DNC registry to centrally assist in the filtering of numbers and checking with the national DNC registry. The NUS DNC registry is managed by the Data Protection Office and all checks with the national DNC registry will be carried out centrally by the Data Protection Office, unless otherwise delegated to a department/unit.

## 6 CLEAR AND UNAMBIGUOS CONSENT

6.1 Individuals may still provide their clear and unambiguous consent to receive Marketing Messages from NUS, notwithstanding that they had registered on the national DNC Registry.

6.2 All individuals who intend to provide such clear and unambiguous consent to NUS shall do so by way of registration at the following website: https://myaces.nus.edu.sg/DNC/. Alternatively, the individual may email dpo@nus.edu.sg to provide his/her clear and unambiguous consent.

## 7 WITHDRAWL OF CONSENT

7.1 Note that the individual can at any time withdraw such consent that he had previously given to NUS.

7.2 If you receive any request for withdrawal of consent by an individual to receiving Marketing Messages, you must immediately act upon it by directing the individual to withdraw his/her consent at the following website https://myaces.nus.edu.sg/DNC/, or by emailing dpo@nus.edu.sg

## 8 BREACH OF DNC REGIME/FRAMEWORK

Should you cause NUS to be in breach of the requirements of the PDPA relating to the sending of Marketing Messages as a result of your failure to strictly adhere to this Policy Document or as a result of your action or omission, you will be subject to disciplinary proceedings. Additionally, NUS will not hesitate to seek compensation from you for any loss or damage suffered by NUS, arising from your action or omission.

## 9 COMPLAINTS

Staff/Students who are aware of an individual wishing to make a complaint please inform the Data Protection Office immediately at dpo@nus.edu.sg.

## ANNEX A

## NUS TELEMARKETING AUTHORISATION REQUEST FORM

**NUS Telemarketing Authorisation Request Form**

To : Data Protection Officer

1. Brief overview of campaign:
2. Purpose of solicitation:
3. Person responsible for solicitation programme:
4. Period of solicitation:
5. Mode(s) of solicitation :
6. Material(s)/script(s) to be used:
7. Indicate any third party service provider(s) to be used:
8. Telephone number(s) of individuals to be contacted:
9. Source(s) of telephone numbers:

I hereby represent and warrant that the information provided above are accurate and to my best knowledge, and that I have read and understood the provisions as set out in the NUS DNC policy.

Name :

Designation and Faculty/School/Unit/Department :

Date :

Approved by*:

Name :

Designation and Faculty/School/Unit/Department :

Date :

(**to be supported by Deans/Heads of Faculty/School/Unit/Department*)

## APPENDIX 15 - EXCLUSIONS AND EXCEPTIONS TO THE OBLIGATIONS UNDER THE PDPA

### 1 PERSONAL DATA COLLECTED BEFORE 2 JULY 2014

1.1 Staff/Students do not need to obtain fresh consent from an individual if the Staff/Student wishes to continue using the Personal Data for the same original purposes that NUS had collected such Personal Data prior to 2 July 2014.

1.2 If there is a different purpose for the use of the Personal Data, a Staff/Student will need to obtain fresh consent from the data subject.

1.3 When relying on this provision of the PDPA, please note that the scope of the provision is very narrow. According to the literal wording of the provision, NUS can only continue *using* Personal Data that has been collected and only for the particular purposes for which the Personal Data was originally collected for. The provision does not extend specifically to *disclosure* of such Personal Data.

### 2 EXCLUDED PERSONAL DATA - CATEGORIES OF PERSONAL DATA THAT ARE EXCLUDED FROM THE APPLICATION OF THE PDPA

2.1 The PDPA does not apply to, or applies to a limited extent to the following categories of Personal Data:

(i) Business Contact Information

(a) Staff/Students do not need to abide by the data protection principles when dealing with Personal Data that constitutes Business Contact Information ("**BCI**") as defined in the PDPA.

(b) Definition:

The PDPA defines BCI as:

i. an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual; and

ii. not provided by the individual solely for his personal purposes*.

iii. *The definition of BCI is dependent on the purpose for which such contact information is provided by an individual. If the individual provided the work-related contact information solely for his personal purposes, the information may no longer constitute BCI.

(ii) Corporate partners

When dealing with corporate partners, corporate contractors or corporate suppliers, Staff/Students must be mindful that they are dealing with employees of the corporate partners. Personal Data of such employees may not always be BCI. Staff/Students who are in doubt as to whether the Personal Data provided does or does not constitute BCI may contact Data Protection Office.

(iii) Personal Data about an individual who is dead

(a) Individual has been dead for more than 10 years:

PDPA obligations do not apply.

(b) Individual has been dead for 10 years or less:

When Staff/Students deal with Personal Data about an individual who has been dead for 10 years or less, they only need to comply with the PDPA provisions relating to the disclosure and protection of Personal Data, namely:

i. Notification Obligation;

ii. Consent Obligation;

iii. Purpose Limitation Obligation;

iv. Accuracy Obligation; and

v. Protection Obligation.

(iv) Personal Data contained in a record that has been in existence for at least 100 years

PDPA obligations do not apply.

(v) Personal Data that has been truly anonymized (with no possibility of re-identification by any third party that such data may be disclosed to)

PDPA obligations do not apply.

## 3 PDPA (FIRST, SECOND, FIFTH & SIXTH SCHEDULES)

3.1 There are limited exclusions and exceptions under the PDPA pertaining to very specific scenarios, circumstances and/or conditions whereby one or more of the data protection principles would not apply.

3.2 Please refer to the following schedules within the PDPA for more details:

(i) First Schedule – Collection, Use and Disclosure of Personal Data without Consent;

(ii) Second Schedule – Additional Bases for Collection, Use and Disclosure of Personal Data without Consent

(iii) Fifth Schedule – Exceptions from Access Requirement

(iv) Sixth Schedule – Exceptions from Correction Requirement

3.3 Staff/Student's intending to rely on an exception or exclusion must obtain prior approval from the Data Protection Office before relying on any such exception. When obtaining such approval, the Staff/Student must notify Data Protection Office of at least the following:

(i) the Personal Data collected, used or disclosed;

(ii) the exception under which the Staff/Student feels the Personal Data is to be collected, used or disclosed; and

(iii) any supporting documents.

## 4 EXCEPTION: PDNC

Collection, Use and Disclosure of the Personal Data of Staff and Students without consent is only permissible when consent has already been obtained from the relevant Staff or Student pursuant to the Personal Data Notice for Staff or Personal Data Notice for Students respectively (as described in paragraph 16 of this Policy Document).

## APPENDIX 16 - ENGAGEMENT WITH THIRD PARTIES

### 1 DATA INTERMEDIARIES

1.1 Definition

A Data Intermediary is an organisation which processes Personal Data on behalf of NUS.

1.2 NUS remains responsible

1.2.1 With respect to Personal Data processed by a data intermediary on NUS' behalf and for NUS' own purposes, NUS remains responsible for complying with the same obligations of the PDPA as if it were processing the Personal Data by itself.

1.2.2 This effectively means that, in using a data intermediary, NUS remains primarily responsible for the actions and omissions of its data intermediary.

1.3 Written contract (OLA Approval)

1.3.1 Staff/Students must ensure that there is in a place a written contract:

(i) approved by OLA*;

(ii) with appropriate warranties, data protection and non-disclosure clauses, to ensure NUS' compliance with and to limit its liability under the PDPA;

(iii) with adequate language and provisions to protect NUS against claims for any breach of the PDPA which had been caused by the third party.

(iv) *Please consult with OLA for the standard clauses and templates to be used in the various contracts and agreements.

1.3.2 Verbal consent or declaration by the data intermediary is not sufficient or acceptable.

1.4 SOPs

1.4.1 In addition to a written contract, Staff/Students engaging Data Intermediaries should also establish appropriate SOPs for the appointed Data Intermediaries to adhere to when processing the NUS Personal Data and include measures to monitor compliance.

1.4.2 In particular, Staff/Students must ensure that:

(i) the Data Intermediary has proper safeguards in place to protect the NUS Personal Data; and

(ii) the Data Intermediary destroys NUS Personal Data in compliance with the PDPA.

### 2 INDEPENDENT THIRD PARTIES

2.1 Staff/Students must protect Personal Data shared with Independent Third Parties

2.1.1 When Staff/Students disclose Personal Data of an individual to another organisation for that organisation's independent purposes, i.e. an independent third party, there is a risk that such third party may fail to use the Personal Data in compliance with the PDPA. (Example: The third party may use the Personal Data for purposes other than those to which the individual had consented.)

2.1.2 In order to satisfy the Protection Obligation under the PDPA, Staff/Students must ensure that there are safeguards in place to protect such shared Personal Data.

2.2 Written contract (as reviewed by OLA )

2.2.1 Staff/Students must ensure that, prior to the disclosure of Personal Data to the independent third party, there is in a place a written contract:

(i) reviewed by DPO/OLA (as necessary);

(ii) with adequate language and provisions to protect NUS against claims for any breach of the PDPA which had been caused by the third party.

2.2.2 Where a third party refuses to do enter into a written agreement , Staff/Students must not provide them with the Personal Data.

2.3 Public Agencies

(i) There may be instances when public agencies request that certain Personal Data be provided to them.

(ii) The default position is that Staff/Students need to obtain consent from an individual before disclosing that individual's Personal Data to a public agency. However, there are exceptions to when consent is not needed. This would be where:

(a) such disclosure is authorised under other written law; or

(b) pursuant to an exception to the requirement of consent under the PDPA, such as where the disclosure is necessary in the public interest.

(iii) When Staff/Students receive a request from a public agency for disclosure of personal data, immediately notify Data Protection Office and await further instructions. Do not disclose any Personal Data until Data Protection Office has given approval to do so.

2.3.2 Corporate Partners

(i) There may be occasions where corporate partners of NUS wish to insert their marketing and/or informational brochures into the letters NUS intends to send to individuals (whether students, staff or otherwise).

(ii) As NUS may not have obtained the requisite consent from the individuals to send such individuals marketing and/or information brochures of NUS' corporate partners, Staff/Students must not include any marketing and/or informational brochures of NUS' corporate partners in any of NUS' letters to individuals, unless the prior written approval of Data Protection Office has been obtained.

2.3.3 Volunteers

(i) When Staff/Students engage any individuals to participate in volunteer activities, whether on behalf of NUS or otherwise, they shall ensure that:

(a) prior to the commencement of such volunteer activities, the Staff/Student has consulted with OLA on the need for any contract/agreement to be entered into between NUS and the relevant individual(s) and if required by OLA, each individual has entered into such contract with NUS;

(b) prior to the commencement of such volunteer activities, each such individual has accepted and agreed and to be bound by the provisions of this Policy

Document (including the documents set out in paragraph 4.1 above - "Interface with the NUS Data Management Policy & Related Policies") as may be applicable to the circumstances in question; and

(c) in the course of their activities, the respective individuals collect, use, disclose and otherwise manage and treat all Personal Data in compliance with this Policy

## APPENDIX 17 - PERSONAL DATA OF NUS STAFF/STUDENTS

## 1 COLLECTION, USE AND DISCLOSURE OF THE PERSONAL DATA OF STAFF/STUDENT

1.1 NUS collects, uses and discloses the Personal Data of NUS Staff and Students for the purposes listed in the Employee Personal Data Notice and Consent Statements or Student Personal Data Notice and Consent Statements respectively which were sent by the Circular dated 30 June 2014 (as the same may be amended/revised, updated and/or supplemented from time to time) and which Staff/Students have agreed to and accepted as part of their employment/enrolment with NUS. These statements can be found for Staff at the NUS Staff Portal and for Students at the NUS Student Portal.

1.2 NUS respects the confidentiality of the Personal Data provided by Staff/Students.

1.3 In that regard, NUS will not disclose any Personal Data of Staff/Students to any third parties without first obtaining the express consent of Staff/Students permitting NUS to do so. However, NUS may disclose the Personal Data of Staff/Students to third parties without first obtaining their consent in certain situations, including, without limitation, the following:

(i) the disclosure is required based on the applicable laws and/or regulations;

(ii) the purpose of such disclosure is clearly in the interests of the Staff/Student and consent cannot be obtained in a timely way;

(iii) the disclosure is necessary to respond to an emergency that threatens the life, health or safety of the Staff/Student or another individual;

(iv) there are reasonable grounds to believe that the health or safety of the Staff/Student or another individual will be seriously affected and consent for the disclosure of the data cannot be obtained in a timely way, provided that NUS shall, as soon as may be practicable, notify the Staff/Student of the disclosure and the purposes of the disclosure;

(v) the disclosure is necessary for any investigation or proceedings;

(vi) the Personal Data is disclosed to any officer of a prescribed law enforcement agency, upon production of written authorisation signed by the head or director of that law enforcement agency or a person of a similar rank, certifying that the Personal Data is necessary for the purposes of the functions or duties of the officer; and/or

(vii) the disclosure is to a public agency and such disclosure is necessary in the public interest.

1.4 The instances listed above are not intended to be exhaustive. For an exhaustive list of exceptions, Staff/Students are encouraged to peruse the PDPA which is publicly available at http://statutes.agc.gov.sg.

1.5 In all other instances of disclosure of Personal Data to third parties with the express consent of Staff/Students, NUS will provide for adequate forms of protection over such personal data and confidentiality and security in the handling and administration of the Personal Data of Staff/Students by such third parties in compliance with the PDPA and the data protection policies of NUS.

## 2 REQUEST FOR ACCESS, CORRECTION AND/OR WITHDRAWAL OF CONSENT FOR THE PERSONAL DATA OF STAFF/STUDENTS

2.1 Staff/Students may request to access and/or correct the Personal Data currently in NUS' possession or withdraw their consent for the collection, use and/or disclosure of their Personal Data in NUS' possession or under NUS' control at any time by submitting their request to the NUS Data Protection Office.

2.2 Access

For a request to access their Personal Data, NUS will provide Staff/Students with the relevant Personal Data within a reasonable time from such a request being made.

2.3 Correction

(i) For a request to correct Personal Data, NUS will process the request by Staff/Students, including undertaking necessary verification activities, as soon as practicable after the request has been made.

(ii) NUS will send the corrected Personal Data to other organisations to which the Personal Data was disclosed by NUS within a year before the date the correction was made, unless that other organisation does not need the corrected Personal Data for any legal or business purpose, or if the Staff/Student so consents, only to specific organisations to which the Personal Data was disclosed by NUS within a year before the date the correction was made.

(iii) NUS may charge Staff/Students a reasonable fee for the handling and processing of their requests to access and/or correct their Personal Data, but Staff/Students will be notified in advance of such costs.

2.4 Withdrawal of consent

(i) For a request to withdraw consent, NUS will process the request by Staff/Students within a reasonable time from such a request for withdrawal of consent being made.

(ii) Requests for withdrawal of consent may adversely impact the relationship of the Staff/Students with NUS and Staff/Students will be notified in advance of such impacts.

2.5 Administration and Management of the Personal Data of Staff/Students

2.5.1 Accuracy

NUS will take appropriate measures to keep the Personal Data of Staff/Students accurate, complete and updated.

2.5.2 Protection

(i) NUS will also take reasonable efforts to take appropriate precautions and preventive measures to ensure that the Personal Data of Staff/Students is adequately protected and secured.

(ii) Appropriate security arrangements will be taken to prevent any unauthorized access, collection, use, disclosure, copying, modification, leakage, loss, damage and/or alteration of the Personal Data of Staff/Students.

(iii) However, NUS cannot assume responsibility for any unauthorized use of the Personal Data of Staff/Students by third parties which are wholly attributable to factors beyond its control.

2.5.3 Retention

NUS will take reasonable efforts to ensure that the Personal Data in its possession or under its control is destroyed and/or anonymized as soon as it is reasonable to assume that:

(i) the purpose for which that personal data was collected is no longer being served by the retention of such Personal Data; and

(ii) retention is no longer necessary for any other legal or business purposes.

## APPENDIX 18 - ROLES AND RESPONSIBILITIES

### 1 DATA PROTECTION OFFICER

| | |
|---|---|
| **Identity** | The DPO refers to the individual as determined by the Senior Management |
| **Role** | The role of the DPO is as the main contact person for PDPA related matters |
| **Responsibilities** | The responsibilities of the DPO shall include:<br><br>(i) Advice:<br><br>Advising management on issues and enquiries relating to the management and use of Personal Data.<br><br>(i) Training:<br><br>Conducting internal training and workshops on the data protection obligations under the PDPA for persons within the University.<br><br>(ii) Liaising with PDPC:<br><br>Liaising with the PDPC on data protection matters where necessary. |

### 2 PDPA POCS

| | |
|---|---|
| **Identity** | A senior staff appointed by the respective Heads as the Point-of-Contact to support the Data Protection Office on compliance with the PDPA in NUS<br><br>For the avoidance of doubt, whilst the PDPA POC may delegate some of their duties to other Staff, they remain responsible for all the responsibilities set out in Appendix 18 as well as the actions taken by such other Staff. |
| **Role** | (i) Support the Data Protection Office on compliance with the PDPA in NUS<br>(ii) The key contact person for Personal Data related matters of the department<br>(iii) Ensures general applicable Personal Data protection legislations compliance, management and procedural responsibilities within the department |
| **Responsibilities (non-exhaustive)** | The responsibilities of the POC shall include:<br><br>(i) Compliance with Personal Data protection legislation applicable to the University:<br><br>(a) Ensure compliance with applicable Personal Data protection legislation when developing and implementing the Personal Data related operational practices and procedures of their respective business units/ departments<br><br>(b) Monitor and ensure compliance by Staff/Students within their respective business units/departments with all prescribed |

| | |
|---|---|
| | procedures and applicable Personal Data protection requirements<br><br>(c) Conduct regular Personal Data protection compliance assessment within their respective business units/departments<br><br>(ii) Operational supervision<br><br>Managing and resolving any Personal Data queries and issues relating to routine operations within the business units (e.g. requests for access to or correction of Personal Data etc.)<br><br>(iii) Education & Communication<br><br>Conduct regular sessions with Staff/Students within their business units to ensure that Staff/Students are familiar with and adhere to all internal policies and procedures for compliance with the applicable Personal Data protection legislations requirements<br><br>(iv) Assist the University<br><br>Provide any input and assistance as may be required by the Office of Risk Management and Compliance / Data Protection Office in the event of Personal Data related issues/complaints.<br><br>(v) Queries:<br><br>Advise their respective business units on Personal Data protection related issues and queries. |

## 3 STAFF/STUDENTS

| | |
|---|---|
| **Responsibilities** | Be fully aware of and comply with the obligations and requirements under this Policy:<br><br>(i) any applicable policy documents or requirements relating to the proper use and management of Personal Data, as may be issued and/or amended from time to time; and<br>(ii) all PDPA Legislation,<br><br>with regards to any Personal Data that they handle in the course of their daily operational activities for NUS and/or in the course of their employment) |

## APPENDIX 19 - PDPC INVESTIGATIONS/RAIDS

**1 IN THE EVENT THAT REPRESENTATIVES OF THE PDPC ARRIVE AT NUS FOR AN INVESTIGATIVE PURPOSE, STAFF/STUDENTS SHOULD BE COMPLYING WITH THE FOLLOWING PRINCIPLES AND PROCEDURES:**

(i) Staff/Students must allow PDPC representatives entry and immediately inform the DPO.

(ii) In the event that DPO (or a representative from Data Protection Office) is not contactable, contact a member from OLA, or the Office of Deputy President (Administration).

(iii) In line with the University's uncompromising policy to cooperate with the PDPC and such other regulatory authorities. Staff/Students must show a willingness to cooperate with the PDPC's investigations and should politely refer all questions from the PDPC to the DPO (or a representative from Data Protection Office).

(iv) The PDPC investigators have extensive powers and can seek information or documents from Staff/Students.

(v) Until the DPO (or a representative from Data Protection Office) or NUS' legal counsel or some other senior management officer of NUS arrives to deal with the PDPC investigators, Staff/Students should as far as reasonably possible, politely defer any answering of questions or provision of information till any of the aforementioned arrive. If this is not possible, then Staff/Students should make a mental note of the answers and information provided and thereafter inform the DPO (or a representative from Data Protection Office) of the answers and information provided.

(vi) Any PDPC investigator who wants to interview or collect data or documents should be told by Staff/Students that they will cooperate, but Staff/Students should politely request that DPO (or a representative from Data Protection Office) and / or Legal Counsel from OLA be present at any interview or production of information.

(vii) A person who neglects or refuses to comply with an order to appear before the PCPC, or without reasonable excuse neglects or refuses to furnish any information or produce the documents requested, or otherwise obstructs the investigation by the PDPC, may be personally liable to a fine and/or imprisonment. Staff/Students must not:

(a) destroy/ tamper/alter documents;

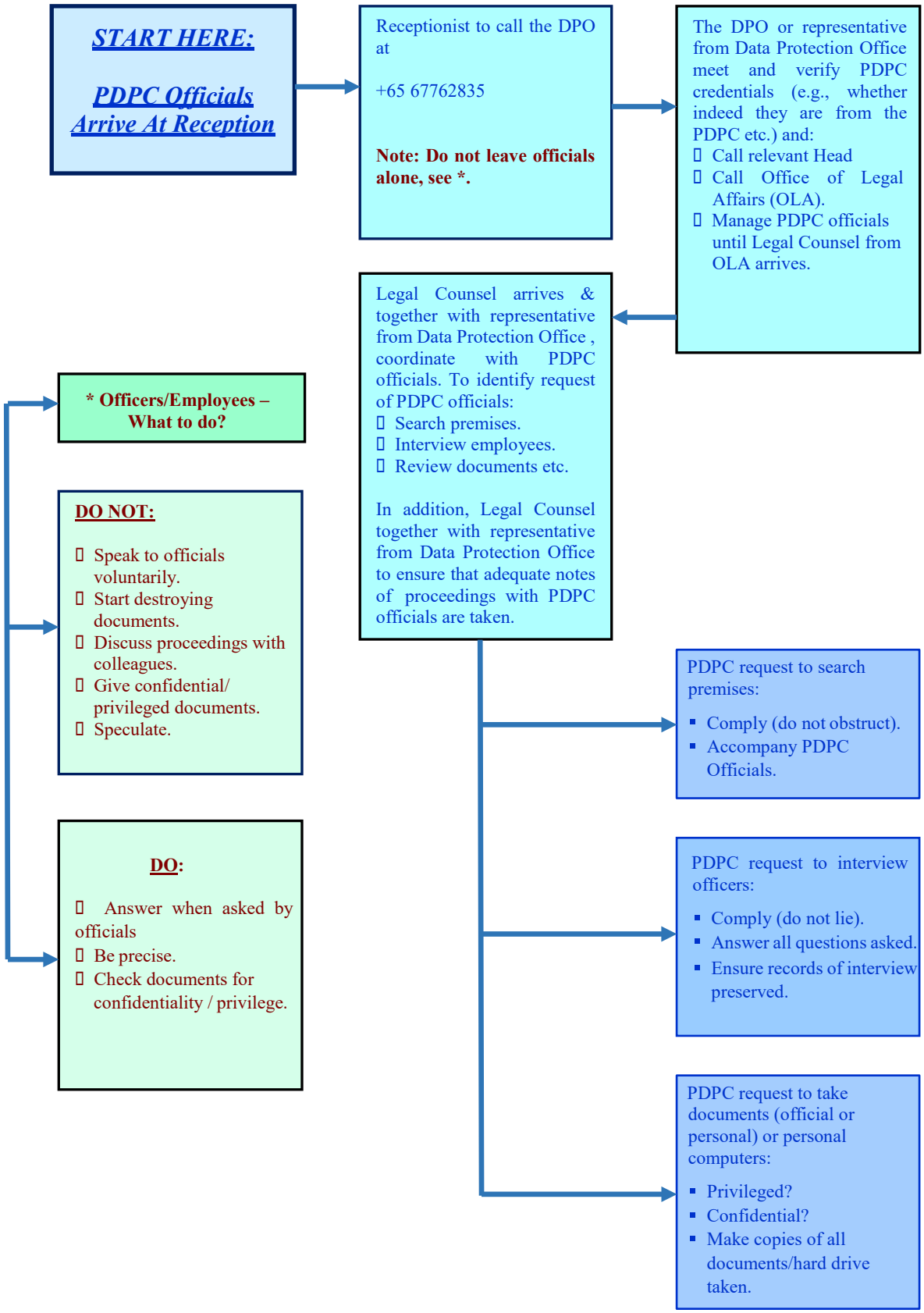
(b) lie or provide false or misleading information;

(c) refuse to provide information or documents requested from you (unless protected by legal privilege); and

(d) obstruct, hinder or delay an investigator who has a right to enter the premises.

(viii) A flowchart is provided below on the appropriate steps to take during an investigation. Staff/Students are expected to be familiar with the flowchart and to refer to it as and when necessary.

## STEPS TO TAKE DURING AN INVESTIGATION/RAID



## APPENDIX 20 - EU GENERAL DATA PROTECTION REGULATION (GDPR)

*Please note in the significant majority of cases, GDPR does not apply to NUS's processing of personal data, even where that processing relates to data subjects in the UK or the EU. As such this section, and any section setting out rights for UK and EU data subjects, will not apply to most of NUS's processing activities. However, on some rare occasions GDPR might apply to limited processing (e.g. potentially, although again rarely, where NUS is offering goods or services to UK or EU data subjects and the GDPR applies pursuant to its territorial application clauses) and as such this Appendix sets out the required GDPR transparency information.

### 1 INTRODUCTION TO THE GDPR

1.1 Overview Of The GDPR

1.1.1 The General Data Protection Regulation ("**GDPR**") is a legal framework for the processing of personal data by organisations based in the European Economic Area "**EEA**") and, where it has extra-territorial effect, outside of the EEA (as is the case with NUS). It sets out the principles for personal data processing and the rights of the individual (known under the GDPR as the "data subject"), while also imposing fines that can (depending on the nature of the breach) either be fixed amounts or revenue-based.

1.1.2 The GDPR came into effect on 25 May 2018. It is largely seen as the biggest effort to protect the personal data of individuals to date, and is therefore significant.

1.1.3 NUS seeks to comply with GDPR requirements where they apply to its activities. As further described in this Appendix, the financial consequences of not complying with the GDPR can be very severe. As such, Staff/Students should have regards to the requirements set out in this Appendix when processing personal data subject to the GDPR.

1.1.4 To the extent that GDPR applies to NUS's processing of personal data, the key obligations under the GDPR to be observed by NUS are as set out in this Appendix. Whilst GDPR requirements are applicable to NUS as the organisation processing personal data, it is the responsibility of all Staff/Students to ensure compliance with the requirements set out in this Appendix.

1.2 Applicability Of The GDPR

1.2.1 The GDPR has "extra-territorial" effect. This means that it can apply to NUS even though NUS is not established in the European Union or the European Economic Area ("EEA").

1.2.2 The GDPR will apply when NUS processes the personal data of data subjects located in the EEA AND the processing activities are related to either:

(i) the offering of goods or services to such data subjects; or

(ii) NUS monitors the behaviour of those data subjects as far as their behaviour takes place in the EEA

(in each case, "**GDPR Processing**").

1.2.3 "**Processing**" is defined in the GDPR as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". In other words, "processing" captures almost any activity NUS carries out in relation to personal data.

1.3 Personal Data Under The GDPR

1.3.1 Personal data under the GDPR (and in relation to GDPR Processing) is defined as "any information relating to an identified or identifiable natural person", where "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". Personal data does not include data where the identity of an individual has been permanently removed.

1.3.2 As a rule of thumb, if something constitutes "Personal Data" under the PDPA, it will also constitute personal data under the GDPR.

1.4 Special Categories of Personal Data under the GDPR

1.4.1 The GDPR also introduces a category of personal data that is considered to be more sensitive and where processing is only allowed under a more limited set of circumstances (known as "**Special Categories of Personal Data**").

1.4.2 The Special Categories of Personal Data comprise personal data revealing any of the following:

(i) racial or ethnic origin,

(ii) political opinions,

(iii) religious or philosophical beliefs,

(iv) trade union membership,

(v) genetic data,

(vi) biometric data,

(vii) data concerning health, or

(viii) data concerning a natural person's sex life or sexual orientation.

1.4.3 NUS may be collecting some Special Categories of Personal Data in limited circumstances. Please see **Section 8** below for an overview of the additional requirements that apply to the limited situations in which NUS collects and processes Special Categories of Personal Data.

1.5 Importance Of The GDPRs

1.5.1 If NUS does not comply with the GDPR in relation to the GDPR Processing, it can be subject to sanctions by the relevant supervisory authority (which, in most cases, will be the data protection regulator of the country the Personal Data originated from). Such sanctions can include warnings or reprimands, bans on certain GDPR Processing and administrative fines.

1.5.2 Any administrative fine imposed under the GDPR has to be "effective, proportionate and dissuasive" in relation to the individual case involved. When determining the level of fine, the relevant supervisory authority needs to take into consideration a number of factors including the nature, gravity and duration of the non-compliance, any action taken to mitigate the damage suffered by the affected individuals, and any relevant previous non-compliance.

1.5.3 The maximum administrative fine under the GDPR can be up to €20 million or 4% of the total worldwide annual revenue of NUS of the preceding financial year, whichever is higher.

1.5.4 For these reasons, it is key for Staff/Students to comply with the requirements set out in this Appendix.

1.6 "Controllers" And "Processors" Under The GDPR

1.6.1 The GDPR applies to both "controllers" and "processors". "Controllers" are defined in the GDPR as natural or legal persons that "determine the purposes and means of the processing of personal data", and "processors" are defined in the GDPR as "natural or legal persons which process personal data on behalf of a controller". "Processors" are, therefore, somewhat akin to "data intermediaries" under the PDPA.

1.6.2 NUS will in most cases be a controller in relation to the GDPR Processing and it is safe for Staff/Students to assume so. This is because NUS typically determines the "why" and the "how" of the processing of personal data, rather than simply processing personal data on behalf of someone else. Unless otherwise specified, this Appendix assumes that NUS is acting as controller – but see below for details of the rules that apply to NUS where it acts as a processor.

1.7 Determining Whether NUS Is A Controller, A Joint Controller Or A Processor

1.7.1 Staff/Students must use the following checklists to determine whether NUS is a controller, a joint controller, or a processor in different situations. The more ticks in the boxes, the more likely NUS is to fall within the relevant category. However, it is not necessary for every box in a category to be ticked, in order to fall within that category.

***Is NUS a controller?***

☐ We decided to collect or process the personal data.

☐ We decided what the purpose or outcome of the processing was to be.

☐ We decided what personal data should be collected.

☐ We decided which individuals to collect personal data about.

☐ We obtain a commercial gain or other benefit from the processing, except for any payment for services from another controller.

☐ We are processing the personal data as a result of a contract between us and the data subject.

☐ The data subjects are our employees.

☐ We make decisions about the individuals concerned as part of or as a result of the processing.

☐ We exercise professional judgement in the processing of the personal data.

☐ We have a direct relationship with the data subjects.

☐ We have complete autonomy as to how the personal data is processed.

☐ We have appointed the processors to process the personal data on our behalf.

***Is NUS a joint controller?***

☐ We have a common objective with others regarding the processing.

☐ We are processing the personal data for the same purpose as another controller.

☐ We are using the same set of personal data (eg one database) for this processing as another controller.

☐ We have designed this process with another controller.

☐ We have common information management rules with another controller.

***Is NUS a processor?***

☐ We are following instructions from someone else regarding the processing of personal data.

☐ We were given the personal data by a customer or similar third party, or told what data to collect.

☐ We do not decide to collect personal data from individuals.

☐ We do not decide what personal data should be collected from individuals.

☐ We do not decide the lawful basis for the use of that data.

☐ We do not decide what purpose or purposes the data will be used for.

☐ We do not decide whether to disclose the data, or to whom.

☐ We do not decide how long to retain the data.

☐ We may make some decisions on how data is processed, but implement these decisions under a contract with someone else.

☐ We are not interested in the end result of the processing

1.8 Responsibilities As A Controller

1.8.1 If NUS is acting as a controller, it shoulders the highest level of compliance responsibility under the GDPR – it must comply with, and demonstrate compliance with, all the data protection principles as well as the other GDPR requirements. NUS is responsible for ensuring that our processing – including any processing carried out by a processor on its behalf – complies with the requirements described in this Appendix, which (for ease of reference) comprise the following:

(i) establish a lawful basis for the processing;

(ii) comply with the GDPR data protection principles;

(iii) vet (and remain liable for) any third-party data processors engaged by it;

(iv) ensure that personal data is properly secured and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage; and

(v) protect and give effect to the rights of data subjects under the GDPR.

1.8.2 As a controller, NUS can ultimately be held liable for both its own compliance and the compliance of its processors. In other words, if NUS is controller, it cannot "outsource" compliance to a processor, although it can seek some contractual protections to manage its risk. Indeed, the GDPR places further obligations on controllers to ensure that their contracts with the processors comply with the GDPR, as described in **Section 3** below.

1.9 Responsibilities As A Joint Controller

In some ways, NUS's responsibilities are the same as that of a controller. However, there are some additional responsibilities:

1.9.1 **Obligations of joint controllers:** NUS must decide with our fellow joint controllers as to who will carry out which controller obligation under the GDPR. However, regardless of those arrangements, each controller remains responsible for complying with all the obligations of controllers under the GDPR.

1.9.2 **Transparent arrangement:** Joint controllers are not required to have a contract, but there must be a transparent arrangement that sets out agreed roles and responsibilities for complying with the GDPR. In most cases, a contract will be the best way of achieving this. The main points of this arrangement must be notified to the relevant individuals.

1.9.3 **Individuals' rights:** In particular, NUS must decide (and be transparent about) how it will comply with transparency obligations and individuals' rights (see **Section 5** below). NUS may choose to specify a central point of contact for individuals. However, individuals must remain able to exercise their rights against each controller.

1.10 Responsibilities As A Processor

As a processor, NUS will still have various direct legal obligations under the GDPR and can still face direct enforcement action. NUS is also likely to face action under the contract it has in place with the data controller. For this reason, the GDPR is still highly relevant and important, even where NUS acts as a processor. The following is a summary of NUS' responsibilities as a processor:

1.10.1 **Controller's instructions:** NUS must only process the personal data on instructions from the controller (unless otherwise required by law). If NUS acts outside of our instructions or process for our own purposes, it will step outside our role as a processor and become a controller for that processing.

1.10.2 **Processor contracts:** NUS must enter into a binding contract with the controller. This must contain a number of compulsory provisions, that must be complied as a processor under the contract. See **Section 3** below for more information.

1.10.3 **Sub-processors:** NUS must not engage another processor (i.e. a sub-processor) without the controller's prior specific or general written authorisation (typically under the contract it has in place with the controller). If authorisation is given, NUS must put in place a contract with the sub-processor, following terms that offer an equivalent level of protection for the personal data, as those in the contract between NUS and the controller.

1.10.4 **Security:** NUS must implement appropriate technical and organisational measures to ensure the security of personal data, including protecting against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.

1.10.5 **Notification of personal data breaches:** if NUS becomes aware of a personal data breach, it must notify the relevant controller without undue delay. Most controllers will expect to be notified immediately, and may contractually require this, as they only have a limited time in which to notify the supervisory authority. NUS must also assist the controller in complying with its obligations regarding personal data breaches. See **Section 7** below for more information.

1.10.6 **Notification of potential data protection infringements:** NUS must notify the controller immediately if any of the controller's instructions would lead to a breach of the GDPR.

1.10.7 **Accountability obligations:** NUS must comply with certain GDPR accountability obligations, such as maintaining records. See **Section 3** below for more information.

1.10.8 **International transfers:** the GDPR's prohibition on transferring personal data outside the EEA applies equally to processors as it does to controllers. This means NUS must ensure that any transfer from within to outside the EEA is authorised by the controller and complies with the GDPR's transfer provisions. See **Section 6** below for more information.

1.10.9 **Co-operation with supervisory authorities:** as a processor, NUS is also obliged to cooperate with supervisory authorities to help them perform their duties.

1.11 Lawful Basis for GDPR Processing

1.11.1 Under the GDPR, all personal data in relation to GDPR Processing has to be processed lawfully, fairly and in a transparent manner. Processing is only considered lawful if there is a lawful basis (also known as a 'legal basis') for doing so under the GDPR, and the applicability of such lawful basis must be able to be demonstrated.

1.11.2 When considering a new processing activity which is subject to GDPR requirements, it is the responsibility of Staff/Students to establish a lawful basis for that new processing activity.

1.11.3 There are six lawful bases for GDPR Processing. These are listed below, together with a brief summary of the requirements for relying on each of the lawful bases.

| **Principle** | **Key requirements** |
|---|---|
| **Lawfulness, fairness and transparency of processing** | (i) There needs to be a lawful basis for collecting and using personal data (for example as a result of consent or the legitimate interests of NUS).<br>(ii) Personal data must only be used in a way that is fair, and in particular that personal data must not be processed in a way that is unduly detrimental, unexpected or misleading to the individuals concerned. Personal data may sometimes be used in a way that negatively affects an individual without this necessarily being unfair. What matters is whether or not such detriment is justified. For example, where personal data is collected to assess whether an individual has been making timely repayments of his debt liabilities, the information is being used in a way that may cause detriment to the individual involved, but the proper use of personal data for this purpose will not be unfair.<br>(iii) NUS must be clear, open and honest with individuals from the start about how their personal data will be used. For example, NUS needs to tell individuals about their processing, through an external privacy policy, in a way that is easily accessible and easy to understand. |
| **Purpose limitation** | Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means that NUS must be clear about what its purposes for processing are from the start.<br><br>These purposes must be recorded and specified in external privacy information for individuals. NUS can only use the personal data for a new purpose if either this is compatible with the original purpose, consent is obtained, or if there is a clear basis in law to do so. |
| **Data minimisation** | (i) Personal data collection must be adequate and sufficient to properly fulfil the stated purposes of processing.<br>(ii) Personal data collected must be relevant to, and have a rational link to, those purposes of processing.<br>(iii) Personal data collection must be limited to what is necessary – NUS must not hold more than what is needed for those purposes.<br>(iii) |
| **Accuracy of data** | (i) Personal data collected and processed must be accurate and, where necessary, kept up to date. This means that NUS must take all reasonable steps to ensure the personal data it holds is not incorrect or misleading as to any matter of fact. If NUS discovers that the |

| | | |
|---|---|---|
| | | personal data is incorrect or misleading, it must take reasonable steps to correct or erase it as soon as possible. |
| | (ii) | Any challenges to the accuracy of personal data by a data subject needs to be carefully considered. |
| **Storage limitation** | (i) | NUS must not keep personal data for longer than needed. |
| | (ii) | NUS needs to think about – and be able to justify – how long it keeps personal data. This will depend on the purposes for holding the data in the first place. |
| | (iii) | NUS needs a policy setting standard retention periods wherever possible, to comply with documentation requirements. |
| | (iv) | NUS must periodically review the data it holds, and erase or anonymise it when the data is no longer needed. |
| | (v) | NUS must carefully consider any challenges to its retention of data. |
| **Integrity and confidentiality of data** | (i) | Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This means that appropriate security measures need to be put in place to protect the personal data NUS holds. |
| | (ii) | NUS must write security procedures for employees to follow, organise employee training, check that security procedures are actually being followed and investigate security incidents when they occur. |
| **Accountability** | (i) | NUS must be responsible for, and be able to demonstrate compliance with, the above six principles. |
| | (ii) | NUS must put written contracts in place with organisations that process personal data on its behalf, maintain documentation on their processing activities, carry out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests, and adhere to relevant codes of conduct and signing up to certification schemes. |

## 2 DATA PROTECTION PRINCIPLES

There are seven key principles under the GDPR that inform the data protection obligations therein. These key principles are:

| **Principle** | **Key requirements** | |
|---|---|---|
| **Lawfulness, fairness and transparency of processing** | (i) | There needs to be a lawful basis for collecting and using personal data (for example as a result of consent or the legitimate interests of NUS). |
| | (ii) | Personal data must only be used in a way that is fair, and in particular that personal data must not be processed in a way that is unduly detrimental, unexpected or misleading to the individuals concerned. Personal data may sometimes be used in a way that negatively affects an individual without this necessarily being unfair. What matters is whether or not such detriment is justified. For example, where |

| | | |
|---|---|---|
| | | personal data is collected to assess whether an individual has been making timely repayments of his debt liabilities, the information is being used in a way that may cause detriment to the individual involved, but the proper use of personal data for this purpose will not be unfair. |
| | (iii) | NUS must be clear, open and honest with individuals from the start about how their personal data will be used. For example, NUS needs to tell individuals about their processing, through an external privacy policy, in a way that is easily accessible and easy to understand. |
| **Purpose limitation** | Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means that NUS must be clear about what its purposes for processing are from the start.<br>These purposes must be recorded and specified in external privacy information for individuals. NUS can only use the personal data for a new purpose if either this is compatible with the original purpose, consent is obtained, or if there is a clear basis in law to do so. | |
| **Data minimisation** | (i) | Personal data collection must be adequate and sufficient to properly fulfil the stated purposes of processing. |
| | (ii) | Personal data collected must be relevant to, and have a rational link to, those purposes of processing. |
| | (iii) | Personal data collection must be limited to what is necessary – NUS must not hold more than what is needed for those purposes. |
| **Accuracy of data** | (i) | Personal data collected and processed must be accurate and, where necessary, kept up to date. This means that NUS must take all reasonable steps to ensure the personal data it holds is not incorrect or misleading as to any matter of fact. If NUS discovers that the personal data is incorrect or misleading, it must take reasonable steps to correct or erase it as soon as possible. |
| | (ii) | Any challenges to the accuracy of personal data by a data subject needs to be carefully considered. |
| **Storage limitation** | (i) | NUS must not keep personal data for longer than needed. |
| | (ii) | NUS needs to think about – and be able to justify – how long it keeps personal data. This will depend on the purposes for holding the data in the first place. |
| | (iii) | NUS needs a policy setting standard retention periods wherever possible, to comply with documentation requirements. |
| | (iv) | NUS must periodically review the data it holds, and erase or anonymise it when the data is no longer needed. |
| | (v) | NUS must carefully consider any challenges to its retention of data. |
| **Integrity and confidentiality of data** | (i) | Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This means that appropriate security measures need to be put in place to protect the personal data NUS holds. |

| | | |
|---|---|---|
| | (ii) | NUS must write security procedures for employees to follow, organise employee training, check that security procedures are actually being followed and investigate security incidents when they occur. |
| **Accountability** | (i) | NUS must be responsible for, and be able to demonstrate compliance with, the above six principles. |
| | (ii) | NUS must put written contracts in place with organisations that process personal data on its behalf, maintain documentation on their processing activities, carry out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests, and adhere to relevant codes of conduct and signing up to certification schemes. |

## 3 ACCOUNTABILITY AND GOVERNANCE

3.1 Under the accountability principle, NUS should take responsibility for its GDPR Processing and compliance with the other data protection principles under the GDPR. This principle also requires NUS to have appropriate measures and records in place to be able to demonstrate its GDPR compliance generally.

3.2 Third Party Processors

When NUS enters into a controller-processor arrangement, whether it acts as controller or processor, NUS will need to put in place a written contract that sets out each party's responsibilities and liabilities ("**Data Processing Addendum**"). Such contracts must include the following specific terms:

3.2.1 an obligation to only process the relevant personal data in accordance with NUS's document instructions;

3.2.2 an obligation to ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

3.2.3 an obligation to take all security measures to protect the personal data in accordance with the requirements of the GDPR;

3.2.4 an obligation to not appoint another processor to process the personal data without NUS's prior approval in writing;

3.2.5 an obligation to assist NUS in responding to requests from the relevant data subjects;

3.2.6 an obligation to assist NUS in addressing data breaches and complying with its reporting obligations under the GDPR;

3.2.7 an obligation to provide all relevant documents to NUS to demonstrate its compliance with the GDPR, and to allow NUS to carry out an audit of its systems; and

3.2.8 an obligation to securely delete the relevant personal data on instructions from NUS.

3.3 Documentation and Records

3.3.1 NUS must maintain a record of all its GDPR Processing. The record will differ slightly depending on whether NUS acts as controller or processor but should contain information such as the purposes of the processing, the categories of personal data being processed, the categories of individuals whose personal data are being processed, and the envisaged time limits for erasure of the personal data.

3.3.2 Documenting all of its GDPR Processing is not only mandatory for compliance but it also allows NUS to be aware of the type of personal data it holds, where it is and what NUS intends to do with it. This makes it easier for NUS to comply with other aspects of the GDPR such as making sure that the personal data NUS holds is accurate and secure.

3.4 Data Protection by Design and Default

3.4.1 NUS must incorporate data protection considerations into its design of new products, processes and systems that use personal data. Data protection by design and default is an integral element of being accountable. This requires NUS to embed data protection into all of NUS's processing operations.

3.4.2 In practice, measures such as applying pseudonymisation techniques, minimising personal data collected and improving security features will be relevant for NUS's compliance with this GDPR requirement.

3.5 Data Protection Impact Assessments

3.5.1 When NUS undertakes GDPR Processing that is likely to result in high risk to an individuals' interests, it would need to, prior to the GDPR Processing, carry out an assessment of the impact of the envisaged GDPR Processing on the protection of personal data ("**DPIA**"). NUS is unlikely to have to carry out a DPIA, but Staff/Students should keep this requirement in mind.

3.5.2 A DPIA will help NUS to identify and minimize data protection risks of any GDPR Processing, and must contain:

(i) a systematic description of the envisaged GDPR Processing and the purposes of this processing, including, where applicable, the legitimate interest pursued;

(ii) an assessment of the necessity and proportionality of the GDPR Processing in relation to the purposes;

(iii) an assessment of the risks to the interests of the individuals affected; and

(iv) the measures envisaged to address the risks, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, taking into account the rights and interests of the individuals affected and other persons concerned.

## 4 SECURITY

4.1 NUS must ensure that personal data is properly secured and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage is particularly important under the GDPR.

4.2 As such, Staff/Students must treat all personal data as highly confidential and ensure that it is not incorrectly disclosed or shared.

## 5 INDIVIDUALS' RIGHTS

Under the GDPR, individuals have a number of rights in relation to their personal data. These rights are set out in the table below.

| **Individuals' Rights** | **Details** | **Timing** |
|---|---|---|
| The right to object to processing | An individual has the right to object to certain types of processing, including **the absolute right to object to the processing of their personal data if it is for direct marketing purposes.**<br><br>If the individual objects, this does not automatically mean that NUS needs to erase the individual's personal data, and in many cases it will be preferable to suppress their details.<br><br>Suppression involves retaining just enough information about them to ensure that their preferences are respected in future. For example, NUS must retain just enough information to note that they object to direct marketing. | <u>Deadline</u><br><br>Within one month.<br><br><u>Extension of Time</u><br><br>NUS can extend the time to respond to an objection by a further two months if:<br><br>(i) the request is complex; or<br><br>(ii) NUS has received a number of requests from the individual.<br><br>NUS must:<br><br>(i) let the individual know within one month of receiving their objection; and<br><br>(ii) explain why the extension is necessary (must have very good reasons for proposing an extension). |
| The right to be informed | An individual has the right to be provided with clear, transparent and easily understandable information about how NUS uses that individual's personal data and his/her rights.<br><br>NUS's external privacy policy, designed for GDPR compliance, addresses the key information requirements in this respect. | <u>Collecting Personal Data directly</u><br><br>Where NUS collects the personal data directly from the individual, it must provide the information at the time that it obtains their personal data.<br><br><u>Collecting Personal Data from another source</u><br><br>Where NUS collects the personal data from another source (i.e. other than from the individual) then it must provide the information:<br><br>(i) within a reasonable period and no later than one month;<br><br>(ii) if it uses the personal data to communicate with the individual, at the time that the first communication is made; or<br><br>(iii) if it envisages disclosure to someone else, at the latest, |

| Individuals' Rights | Details | Timing |
|---|---|---|
| | | when it discloses the personal data. |
| The right of access | An individual has the right to obtain access to his/her own personal data (if NUS is/has been processing it).<br><br>There are no specific parameters as to the time period within which the personal data must have been processed by us. | <u>Deadline</u><br><br>Within one month.<br><br><u>Extension of Time</u><br><br>NUS can extend the time to respond to an objection by a further two months if:<br><br>(i) the request is complex; or<br><br>(ii) it has received a number of requests from the individual.<br><br>NUS must:<br><br>(i) let the individual know within one month of receiving their objection; and<br><br>(ii) explain why the extension is necessary (must have very good reasons for proposing an extension). |
| The right to rectification | An individual is entitled to have his/her personal data corrected if it is inaccurate. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data. | <u>Deadline</u><br><br>Within one month.<br><br><u>Extension of Time</u><br><br>NUS can extend the time to respond to an objection by a further two months if:<br><br>(i) the request is complex; or<br><br>(ii) it has received a number of requests from the individual.<br><br>NUS must:<br><br>(i) let the individual know within one month of receiving their objection; and<br><br>(ii) explain why the extension is necessary (must have very good reasons for proposing an extension). |
| The right to erasure | This is also known as 'the right to be forgotten' and, in simple terms, enables an individual to request the deletion or removal of his/her personal data where | <u>Deadline</u><br><br>Within one month. |

| Individuals' Rights | Details | Timing |
|---|---|---|
| | there is no compelling reason for NUS to keep using it. This is not a general right to erasure and does not apply if processing is necessary for one of the following reasons:<br>(i) to exercise the right of freedom of expression and information;<br>(ii) to comply with a legal obligation;<br>(iii) for the performance of a task carried out in the public interest or in the exercise of official authority;<br>(iv) for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or<br>(v) for the establishment, exercise or defence of legal claims. | <u>Extension of Time</u><br>NUS can extend the time to respond to an objection by a further two months if:<br>(i) the request is complex; or<br>(ii) it has received a number of requests from the individual.<br>NUS must:<br>(i) let the individual know within one month of receiving their objection; and<br>(ii) explain why the extension is necessary (must have very good reasons for proposing an extension). |
| The right to restrict processing | An individual has rights to 'block', suppress or limit further use of his/her personal data. This is an alternative to having the personal data erased, as described above.<br>This may be because they have issues with the content of the information NUS holds or how NUS has processed their data.<br>In most cases, NUS will not be required to restrict the processing of an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.<br>When processing is restricted, NUS can still store that individual's personal data, but may not use it further. | <u>Deadline</u><br>Within one month.<br><u>Extension of Time</u><br>NUS can extend the time to respond to an objection by a further two months if:<br>(i) the request is complex; or<br>(ii) it has received a number of requests from the individual.<br>NUS must:<br>(i) let the individual know within one month of receiving their objection; and<br>(ii) explain why the extension is necessary (must have very good reasons for proposing an extension). |
| The right to data portability | An individual has rights to obtain and reuse his/her own personal data for his/her own purposes across different | <u>Deadline</u><br>Within one month. |

| Individuals' Rights | Details | Timing |
|---|---|---|
| | services. For example, if an individual decides to switch to a new education provider, this right enables him/her to move, copy or transfer his/her personal data easily between NUS's IT systems and the new provider's IT systems, safely and securely, without affecting its usability. | <u>Extension of Time</u><br>NUS can extend the time to respond to an objection by a further two months if:<br>(i) the request is complex; or<br>(ii) it has received a number of requests from the individual.<br>NUS must:<br>(i) let the individual know within one month of receiving their objection; and<br>(ii) explain why the extension is necessary (must have very good reasons for proposing an extension). |
| The right to lodge a complaint | An individual has the right to lodge a complaint about the way NUS handles or processes his/her personal data with that individual's national data protection regulator. NUS will need to deal with any complaint or grievance that an individual has speedily and fairly. See **Section 10** below for more information. | NUS must respond as soon as reasonably practicable.<br>In most cases, NUS should be responding within a couple of days to avoid the matter being escalated. If a Staff/Student receives such a request, they must forward it to the Data Protection Office immediately. |
| The right to withdraw consent | If an individual has given his/her consent to anything NUS does with that individual's personal data, that individual has the right to withdraw his/her consent at any time. This includes (but is not limited to) that individual's right to withdraw consent to NUS using his/her personal data for marketing purposes.<br>NUS must make it as easy for the individual to withdraw consent as it was for them to give consent. | NUS will need to process an individual's request within a reasonable time from such a request for withdrawal of consent being made, and must, thereafter, not collect, use and/or disclose that individual's personal data in the manner stated in his/her request. |
| The right not to be subject to automated decision-making including profiling | The individual has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. It is a | As soon as reasonably practicable.<br>If a Staff/Student receives such a request, they must forward it to the Data Protection Office immediately. |

| Individuals' Rights | Details | Timing |
|---|---|---|
| | safeguard against the risk that a potentially damaging decision is taken without human intervention. This works slightly differently to the other individual rights listed in this table - see **Section 9** below for more information. | |

5.1 Individuals' Requests to Exercise Rights

5.1.1 An individual has the right to contact NUS to exercise any of their rights under the GDPR (as set out in the table above), and these rights often come with short deadlines. Such requests can come through multiple channels, including social medial or email.

5.1.2 NUS should generally act on such requests and provide information and/or updates free of charge, but can charge a reasonable fee to cover NUS's administrative costs for baseless or excessive/repeated requests, or further copies of the same information.

5.1.3 Under the GDPR, NUS is required to act upon the relevant requests "without undue delay", and in any event within the timelines stated above.

5.1.4 In order to ensure compliance with such requirements, Staff/Students should escalate any data subject requests as set out in the table above as soon as possible.

5.2 What You Need To Do When You Receive A Request To Exercise Rights

5.2.1 If a Staff/Student receives a request by an individual to exercise any of their rights under the GDPR, regardless of the channel that it reaches them by, they should contact the Data Protection Office immediately with all relevant details pertaining to such request.

5.2.2 Do not respond to the request until you receive guidance. If Staff/Student has any doubts as to the individual's identity, they can ask them for reasonable information to identify themselves. However, they should not use this as a way of obstructing their request.

## 6 DATA TRANSFERS

6.1 The GDPR restricts the cross-border transfer of personal data in relation to GDPR Processing. These restrictions apply to all transfers, regardless of the size of transfer or how often they are carried out.

6.2 When personal data is transferred out of Singapore in relation to GDPR Processing ("**Restricted Transfer**"), NUS would need to ensure that the rights of individuals under the GDPR are properly protected or one of a limited number of exceptions applies. For the avoidance of doubt, a Restricted Transfer includes a transfer of personal data from one group entity to another group entity.

6.3 Before a Restricted Transfer can be made, NUS has to ensure that proper protections are in place, which needs to be one of the following:

(i) the country where the recipient is based is covered by an EU Commission "adequacy decision", where a finding has been made that the legal framework in place in that

country, territory or sector provides "adequate" protection for individuals' rights and freedoms for their personal data ("**Adequacy Decision**")[1]; or

(ii) that "appropriate safeguards" are in place to ensure that NUS and the recipient are legally required to protect individuals' rights and freedoms for their personal data, which can include either binding corporate rules, which are an internal code of conduct for entities within a group, or standard data protection clauses adopted or approved by the EU Commission ("**Appropriate Safeguards**").

6.4 In the absence of an Adequacy Decision or an Appropriate Safeguard, NUS can make a Restricted Transfer if that Restricted Transfer is covered by one of a limited number of exceptions set out below:

(i) explicit consent by the individual to the Restricted Transfer. This consent needs to be specific and informed (the individual needs to be provided with precise details of the Restricted Transfer and the possible risks of such transfer), and valid consent cannot be obtained for Restricted Transfers in general;

(ii) if the Restricted Transfer is necessary for NUS to perform a contract with the individual, or the implementation of pre-contractual measures taken at that individual's request;

(iii) if the Restricted Transfer is necessary for the conclusion or performance of a contract concluded in the interests of the individual between NUS and another natural or legal person;

(iv) if the Restricted Transfer is necessary for important reasons of public interest;

(v) if the Restricted Transfer is necessary for the establishment, exercise or defense of legal claims;

(vi) if the Restricted Transfer is necessary to protect the vital interests of an individual, where that individual is physically or legally incapable of giving consent;

(vii) if the Restricted Transfer is made from a public register; or

(viii) if NUS is making a one-off Restricted Transfer and it is in its compelling legitimate interests.

## 7 PERSONAL DATA BREACHES

7.1 Personal Data Breaches Under The GDPR

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a personal data breach is more than just about losing personal data.

For example, there would be a personal data breach if:

(i) a Staff/Student who has access and/or control over the personal data discloses that data to a person without proper authorisation, either deliberately or by accident (e.g. by sending it to an incorrect postal address, or attaching an incorrect document to an email);

(ii) a Staff/Student who has access and/or control over the personal data misplaces an unencrypted device or a physical document containing that personal data;

[1] The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protectionf. To access the latest list, see: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

(iii) a Staff/Student who has access and/or control over the personal data uploads that personal data to a webpage (which is publicly available) without proper authorisation; or

(iv) an unauthorised person manages to gain unlawful access to personal data in NUS's systems or devices.

7.2 Reporting Personal Data Breaches To Regulators Under The GDPR

7.2.1 Under the GDPR, NUS needs to notify the relevant data protection regulator within 72 hours of becoming aware of the personal data breach if the breach is likely to result in a risk to individuals' rights and freedoms.

7.2.2 It would be prudent to assume that the "relevant data protection regulator" will be the regulator responsible for the jurisdiction or jurisdictions that are the subject of the personal data breach. In most cases, this would be the jurisdiction or jurisdiction where affected EEA Data Subjects are located. This may in fact involve notifications to multiple regulators. For example, if a personal data breach affected EEA Data Subjects in Germany, France, Spain and the UK, it would be necessary to notify all of the relevant regulators.

7.2.3 In order to determine whether NUS has to make such a breach notification, the likelihood and severity of the resulting risk to individuals' rights and freedoms will need to be established. If there is likely to be a risk to individuals' rights and freedoms then NUS has to notify the relevant data protection regulator. If NUS decides that it does not need to report the breach, it would need to be able to justify this decision, and should document it.

7.2.4 The risk does not need to be a high risk – only a risk. In assessing "risk" to individuals' rights and freedoms, NUS should focus on the potential negative consequences for those individuals. A personal data breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised.

7.2.5 Many data protection regulators provide a standard form for the purpose of notifying personal data breaches, and NUS should identify this from the relevant regulators' websites. For example, the UK's Information Commissioner's Office (ICO) provides a self-assessment process and associated form.

7.3 Reporting Data Breaches To Affected Data Subjects Under The GDPR

7.3.1 Under the GDPR, NUS also needs to notify the affected individuals without undue delay if the breach is likely to result in a high risk to individuals' rights and freedoms.

7.3.2 A 'high risk' means the threshold for informing individuals is higher than for notifying the relevant data protection regulator, as outlined above. Again, NUS should assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring.

7.3.3 There is no fixed definition of "high risk" and this needs to be assessed on a case by case basis. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher.

7.3.4 In such cases, NUS will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. As an example, a breach involving financial information of EEA Data Subjects is likely to result in a high risk to individuals' rights and freedoms because of the potential consequences for those EEA Data Subjects – for example, it may expose them to identity theft and/or fraud, and it may expose them to financial losses.

7.3.5 However, there are no absolute rules for what constitutes "high risk" and this is a matter of interpretation that will need to be confirmed on a case-by-case basis. In borderline cases, it is safest to notify the relevant individuals to avoid an inadvertent breach of the notification obligations.

7.3.6 The wording of this notification will need to be crafted carefully in light of the specific facts of the data breach incident, with input from the legal team and, most likely, other relevant teams, such as the communications, Public Relations and customer services teams.

7.4 Other Steps That Need To Be Taken In Response To A Personal Data Breach

7.4.1 NUS need to record all breaches, regardless of whether or not they need to be reported to the relevant data protection regulator or affected individuals. Such records must include the facts relating to the breach, its effects and the remedial action taken by NUS.

7.4.2 In addition, NUS should investigate whether or not the breach was a result of human error or a systemic issue and determine how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

7.5 What You Need To Do Upon A Personal Data Breach

If you know or suspect that a data breach has occurred or may occur, Staff/Students should:

7.5.1 not attempt to investigate the matter yourself – do not make any notifications to affected individuals or the relevant data protection regulators yourself;

7.5.2 report the actual or suspected breach to the Data Protection Office immediately; and

7.5.3 preserve all evidence related to the actual or suspected breach.

## 8 SPECIAL CATEGORIES OF PERSONAL DATA

8.1 Special Categories Of Personal Data Under The GDPR

8.1.1 See **Section 1** above in respect of what constitutes Special Categories of Personal Data ("Special Categories of Personal Data under the GDPR").

8.1.2 "Special Categories of Personal Data" is a subset of personal data under the GDPR. This means that all of the requirements outlined in this Appendix apply as a baseline for the processing of Special Categories of Personal Data.

8.1.3 However, in addition to those baseline requirements, there are <u>further requirements</u> for the processing of Special Categories of Personal Data that must be met. If the requirements are not met, then the processing of Special Categories of Personal Data is prohibited under the GDPR, so it is important that NUS meets the relevant requirements.

8.2 Additional Requirements For The Processing Of Special Categories Of Personal Data Under The GDPR

8.2.1 Before NUS processes any Special Categories of Personal Data, it needs to identify a lawful basis for the processing, just as NUS would for any other category of personal data. See **Section 1** above for an overview of the various legal bases.

8.2.2 NUS must also identify a **separate** condition for the processing of the Special Categories of Personal Data. This does not have to be linked to the legal basis that NUS has identified under **Section 1**. For example, if NUS relies on "consent" as the lawful basis as described in **Section 1** above, it is not restricted to only using explicit consent as the separate condition for the processing of Special Categories of Personal Data. NUS must choose whichever condition is the most appropriate in the circumstances – although in many cases there may well be an obvious link between the two.

8.2.3 There are ten conditions for the processing of Special Categories of Personal Data under the GDPR[2]. These conditions are listed below, for completeness, but in virtually all situations, the most relevant condition for the processing of Special Categories of Personal Data by NUS will be based on the explicit consent of the individual.

| Condition | Description under the GDPR |
|---|---|
| **Explicit consent** | Where the individual gives explicit consent to the processing of the Special Categories of Personal Data for one or more specified purposes. |
| **Archiving, scientific or historical research** | Where the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR (which contains further safeguards, such as recommending pseudonymisation), based on certain European Union or Member State laws. |
| **Employment, social security and social protection law** | Where the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of NUS as a data controller, or of the individual, in the field of employment and social security and social protection law, insofar as this is authorized by European Union or Member State laws or collective agreements under Member State. |
| **Vital interests** | Where the processing is necessary to protect the vital interests of the individual or of another natural person where the individual is physically or legally incapable of giving consent. |
| **Public data** | Where the processing relates to personal data which are manifestly made public by the data subject. |
| **Legal claims or courts** | Where the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity. |
| **Public interest** | Where the processing is necessary for reasons of substantial public interest, on the basis of certain limited European Union or Member State law with proportionality and other safeguards. |
| **Others** | Where the processing is necessary for the purposes of preventive or occupational medicine, etc.<br><br>Where the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and subject to additional conditions.<br><br>Where the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of certain European Union or Member State laws. |

8.3 Relying On Explicit Consent For The Processing Of Special Categories Of Personal Data

[2] Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. This sets out the general position under the GDPR, which is a sensible, risk-based approach for NUS to apply.

The consent must be unambiguous and involve a clear affirmative action (an opt-in). NUS must not use pre-ticked boxes. Consent must be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

8.4 Criminal Offence Data

8.4.1 Criminal offence data is personal data relating to criminal convictions and offences, or related security measures. this is treated in a similar way to Special Categories of Personal Data, it is regulated slightly differently under the GDPR.

8.4.2 Before processing criminal offence data, and similar to Special Categories of Data, NUS would have to identify a legal basis in exactly the same way as NUS would for any personal data. See **Section 1** above.

8.4.3 NUS would also need to satisfy itself that the processing is authorized by a European Union or Member State law which itself must provide for appropriate safeguards for the rights and freedoms of data subjects. Given that relying on this condition would depend on our interpretation of specific European Union and/or Member State laws, NUS cannot assume that this condition applies without first obtaining specific advice from a law firm in the European Union and/or applicable Member State.

8.5 Other Requirements In Relation To Special Categories Of Personal Data And/Or Criminal Offence Data

8.5.1 Given the risks to EEA Data Subjects that arise from our processing of these highly-sensitive types of personal data, NUS must apply the highest technical and organisational security measures it has in place for this processing.

8.5.2 There are no mandated minimum security measures applicable to these categories of data but, as a rule of thumb, the more sensitive the personal data, the higher the standards of security protection NUS should apply to that personal data.

## 9 AUTOMATED DECISION-MAKING INCLUDING PROFILING

The individual has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. This is a safeguard against the risk that a potentially damaging decision is taken without human intervention.

## 10 COMPLAINTS AND INVESTIGATIONS

10.1 Investigations

10.1.1 Under the GDPR, the relevant data protection regulator has the power to conduct investigations on NUS in relation to its compliance with the GDPR.

10.1.2 If a Staff/Student knows or suspects that an investigation by a relevant data protection regulator has or may commence, they should report this to the Data Protection Office immediately.

10.2 Complaints

10.2.1 Under the GDPR, individuals have the right to lodge a complaint about the way NUS handles or processes his/her personal data with that individual's national data protection regulator.

10.2.2 NUS will need to deal with any complaint or grievance that an individual has speedily and fairly.

10.2.3 If a Staff/Student knows or suspects that an investigation by a relevant data protection regulator has or may commence, they should report this to the DPO immediately.

## 11 EXEMPTIONS

11.1 The exemptions available to NUS (for compliance with the GDPR requirements) are very limited. For completeness, the exemptions available under the GDPR are summarised below but may change in the future.

11.2 EU Member States are allowed to introduce exemptions under the GDPR to the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard, amongst other things:

(i) national security;

(ii) defence;

(iii) public security;

(iv) important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;

(v) the protection of the individual, or the rights and freedoms of others; or

(vi) the enforcement of civil law matters.

(vii) In addition, EU Member States can provide exemptions, derogations, conditions or rules in relation to specific processing activities, including processing that relates to:

(viii) freedom of expression and freedom of information;

(ix) public access to official documents;

(x) national identification numbers; and

(xi) processing of employee data.

11.3 In practice, the exceptions are very limited and it is safest to assume that they will not apply in relation to the GDPR Processing.