NUS DATA MANAGEMENT POLICY 3.0 APPENDICES

Contents

APPENDIX A: DEFINITIONS

This Appendix provides:

(i) The meaning of words and abbreviations used in the DMP.

(ii) A summary of commonly used terms in the DMP.

Administrative Data	University Data that is used for the administration of the University including Personal Data and Analytics Data. Examples include data related to student, staff, alumni, donors and financial records.
Analytics Data	Data that is collected, created or aggregated for analysis, including predictive, forecast and optimisation modelling, to support tactical and strategic decision-making and research purposes in the University. Examples include the collection and analysis of data generated during the student journey and learning process, which is then utilised by the University to improve the quality of teaching and learning.
BCI	Business Contact Information, as defined in the PDPA means "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, not provided by the individual solely for his personal purposes". (PDPA and protection measures for NUS Confidential data do not apply to BCI). Examples include information on NUS business cards such as name, department, designation/title, contact numbers and address, skype and email.
Central Administration	University Administration departments responsible for the administration of the University. Examples include Office of Admissions, Office of Human Resources, Office of Finance and Registrar's Office.
CU	Confidentiality Undertaking to be used for Data Disclosure to External Parties.
Data Classification	The classification or labelling of University Data as *NUS Confidential, NUS Restricted* or *Unclassified* depending the level of sensitivity and impact to the University.
Data Custodian	An NUS Staff member (typically playing the role of an IT function) who owns the technical accountability for University Data and is responsible for the technical management of the data.

Data Disclosure	The act of disclosing or making available University Data to External Parties; distinguished from the act of Data Sharing (as defined below) with Data Users.
Data Incident	Incidents of Data Loss or Data Leakage.
Data Leakage	The situation when any University Data is intentionally or unintentionally accessed by or made available to unauthorised parties.
Data Loss	The situation when any University Data is completely lost, is no longer accessible, cannot be recovered or retrieved from backup sources, and no other copies or documentation exist such that the data can be recreated.
Data Manager	An NUS staff member (typically at the level of Manager and above or equivalent), appointed by the Data Steward, who has operational-level responsibility for data management activities and assists in day-to-day operational matters relating to University Data in his/her function and department.
Data Owner	NUS who *owns* all University Data.
Data Sharing	The act of sharing or making available University Data to Data Users; distinguished from Data Disclosure (as defined above) to External Parties.
Data Steward	The Head of Department (HOD) who is accountable for University Data within his/her functional area and department.
Data Users	Any person who has access to University Data to do work for NUS. They include NUS Staff and Non-NUS Staff. The Policy applies to them. They exclude External Parties who do not do any work for NUS.
DPO	Data Protection Officer an NUS staff designated by NUS to be responsible for ensuring compliance with the PDPA.
Enterprise Data Warehouse	Central Analytics Data repository of the University in curated data format and used primarily for administrative purposes. Comprises Detailed Data Stores and Data Marts.
External Parties	Parties whom University Data has been disclosed to, or parties whom the University has received data from. These parties do not access the data to do work for NUS. The Policy does not apply to them. They exclude the Data User whom University Data has been shared and access has been granted to do work for NUS. Examples include NUS/non-NUS students (and their family members), alumni, family members of staff, ex-staff, donors, government agencies, other academic/research institutions, external organisations and any other person whom data will be disclosed to who is not a Data User.
Master Source	Key data sets, as determined by the Data Governance Team, to facilitate a single source of truth for Data Sharing. Examples include Student data (under Registrar's Office) and Staff data (under Office of Human Resources).

NDA	Non-Disclosure Agreement is a legally binding agreement signed between NUS and External Parties or Non-NUS Staff that sets out the confidentiality obligations, purpose and limitations governing the Data Disclosure.
Non-NUS Staff	Individuals who are not employees of NUS but they are Data Users. They include: • NUS and Non-NUS Student assistants, interns, helpers or volunteers (in departments, NUSSU, clubs and societies, halls and residences) • Volunteers • Contractors, vendors, temporary workers • Any others who do work for the University
NUS DMP or DMP	NUS Data Management Policy: the overarching policy for all data management-related documents and activities in the University.
NUS Staff	NUS employees who are Data Users. They include: • NUS Faculty and Staff • Part-time Teaching Staff • Contingent (casual/temporary) Staff
Officer-in-Charge or OIC	An NUS Staff member appointed by the Data Manager to perform the operational user access rights control for the data in application systems under their responsibility.
PDPA	Personal Data Protection Act 2012 and all subsidiary legislation related thereto.
PDPC	Personal Data Protection Commission. The Info-communications Media Development Authority is designated as the PDPC to administer and enforce the Personal Data Protection Act 2012 (PDPA).
Personal Data	As defined in the PDPA means data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access. For example, it includes records of a patient whose condition/ circumstances are so distinctive as to result in that patient being identifiable from the data.
Primary Data Steward	The Data Steward who plays the lead role for a larger application system or data repository with multiple data sources having multiple Data Stewards.
Research DMP	The Research Data Management Policy: a complementing policy to the DMP on the management of Research Data.
Research Data	Any recorded data or information, in all formats, regarding or related to or generated from research conducted by NUS or on behalf of NUS including Personal Data and Analytics Data.

	Examples include research records, presentations, papers, books and abstracts. Please refer to the Research Data Management Policy for the complete detailed definition of Research Data.
Senior Management	NUS leadership team led by NUS President.
System Owner	An NUS staff member (typically at the level of Manager and above or equivalent), appointed by the Data Steward, who has responsibility for the application systems assigned to him/her including providing the business requirements to IT for the development and operations of the application systems, and ensuring the application systems developed by IT enable them to maintain the availability, integrity and security of the data.
Teaching and Instructional Materials	Materials, information and documents created for educational purposes, including any electronic or non-electronic materials used in the pursuit of teaching and learning.
University	The National University of Singapore or NUS.
University Data	Any data or information created, collected, processed, derived or used in any form or medium by the University and its representatives, regardless of where or how it is stored, its mode of transmission, who is using it, or, from where or how its access is gained. It includes both electronic and non-electronic forms of data. It includes Administrative Data and Research Data (both of which include Personal Data and Analytics Data). It excludes Teaching and Instructional Materials. Please refer to **Appendix C** for the Data Classification and Data Stewards of some Pre-defined Key Data Sets.

APPENDIX B: DATA STEWARDSHIP AND USAGE ROLES AND RESPONSIBILITIES

This Appendix provides:

(i) Information on the Data Steward role including the appointment of data-related operational roles: Data Manager and System Owner.

(ii) Instructions to Data Users on use of University Data.

1. Data Stewards

1.1. Data Stewards (Heads of Department) are accountable for University Data within their functional area and provide overall guidance for the processing and use of University Data within their function and department.

1.2. In general, they are responsible for the collection, use, maintenance, disposal and protection of University Data within their function and department. This responsibility also covers University Data shared with or accessed by their department for which they are not the Data Steward.

1.3. Data Stewards will ensure that the necessary data procedures and guidelines are put in place within their function and department. These procedures and guidelines must be aligned with the DMP.

1.4. Data Stewards will ensure that the areas of responsibility for all data-related activities are clearly defined and assigned to specific individuals and groups.

1.5. They appoint Data Managers and System Owners to assist them in the day-to-day operational matters with respect to University Data and application systems respectively. These operational matters include:

(i) Establishing and keeping current data definitions with clearly defined purposes for collection and use;
(ii) Ensuring transparency of use, purpose, interpretation of data to all stakeholders;
(iii) Classifying each data item;
(iv) Taking necessary measures to ensure data quality, accuracy and validity, essential for effective operations and business decision making;
(v) Taking necessary measures to ensure ethical conduct and use (e.g. in the case of human-related analytics initiatives);
(vi) Establishing data control and protection requirements to protect the data against accidental or unlawful loss, as well as unauthorised access, disclosure, copying, use or modification;
(vii) Establishing data viewing, copying, downloading or other access procedures for each database or set of data;
(viii) Defining the criteria for archiving or disposing the data to satisfy legal and business retention requirements and ensuring the data is properly disposed of; and
(ix) Determining, monitoring and reviewing appropriate security requirements.

Additional considerations for Analytics Data

(x) Ensuring any ethical-related analytics must be approved by the business sponsor of the initiative; and

(xi) Providing perspectives on analytics results to be free from biases.

1.6. Should there be multiple Data Stewards involved in a larger application system or data repository with multiple data sources, a Primary Data Steward should be appointed to play the lead role. The lead role should be selected based upon the guiding principles such as accountability for the proportion of data, criticality of data, and extent of need or interest.

1.7. Where data is derived from sources of data under different Data Stewards, the one who requires the derived data will play the role of Primary Data Steward for that derived data.

1.8. The Primary Data Steward and the multiple Data Stewards will determine the rules of engagement (e.g. to approve access, or to identify a Data Manager/System Owner lead).

2. Data Managers

2.1 Data Managers are appointed when University Data needs to be collected and maintained.

2.2 They are NUS staff (typically at the level of Manager and above or equivalent) who have operational-level responsibility for data management activities including creating, updating, archiving, disposing and securing the data, understanding and maintaining the definition, purpose, use and classification of the data, ensuring the quality and accuracy of the data, and authorising access to the data according to the Policy approval process. Their responsibilities also include handling of data sharing with Data Users or data disclosure to External Parties, as well as providing data requirements to System Owners.

2.3 They carry out these responsibilities and develop data procedures and guidelines for their function and department in consultation with the Data Steward.

2.4 The Data Manager function is typically the responsibility of the business unit and not IT support unit. Each University Data item defined should have a corresponding Data Manager responsible.

2.5 The Data Manager may appoint an Officer-in-Charge (OIC) to perform the operational user access rights control for the data in application systems under their responsibility.

3. System Owners

3.1 System Owners are appointed when application systems need to be developed for the collection and maintenance of University Data.

3.2 They are NUS staff (typically at the level of Manager and above or equivalent) who have responsibility for the application systems assigned to them including providing the business requirements to IT for the development and operations of the application systems. They liaise with stakeholders including Data Managers to consolidate business and data requirements. They are responsible for ensuring the application systems developed by IT enable them to maintain the availability, integrity and security of the data.

3.3 They carry out these responsibilities in consultation with the Data Steward.

3.4 The System Owner function is typically the responsibility of the business unit and not the IT support unit. Each application system should have a corresponding System Owner responsible.

4. Data Custodian

4.1 The Data Custodian is responsible for the technical platform hosting University Data including its technology, design, modelling, technical maintenance and support.

4.2 They are NUS Staff (typically playing the role of an IT function) who own the technical accountability for University Data and are responsible for the technical management of the data.

4.3 The Data Custodian does not access production data without proper authorisation from the Data Steward/Data Manager. They may have access to anonymised production data solely for support purposes to resolve issues.

5. Data Users

5.1 A Data User is any person who has access to University Data to do work for NUS. The DMP applies to all Data Users, which include:

<u>NUS Staff</u>

(i) NUS Faculty and Staff
(ii) Part-time Teaching Staff
(iii) Contingent (casual/temporary) Staff

<u>Non-NUS Staff</u>

(iv) NUS and Non-NUS Student assistants, interns, helpers or volunteers (in departments, NUSSU, clubs and societies, halls and residences)
(v) Volunteers
(vi) Contractors, vendors, temporary workers
(vii) Any others who do work for the University

5.2 NUS Staff responsible for the hiring or engagement of Non-NUS Staff must ensure that the Non-NUS Staff are bound by a Non-Disclosure Agreement (NDA) or equivalent terms and conditions. In addition, NUS Staff must ensure the Non-NUS Staff uphold the principles of this DMP and the instructions below on use of University Data.

5.3 NUS Staff must not give NUS Student assistants/interns, helpers or volunteers administrative access to data not intended for students (e.g. access relating to their peers, access for staff only, or access to NUS Confidential data).

5.4 Data Users are expected to follow these instructions on use of University Data:

(i) Data Users who access University Data must only do so for the purpose of conducting University-related business or matters within their scope of work and duties. In the case of data received from External Parties in the course of work, such data must only be used for the purpose agreed with the External Parties and Data Users must comply with the NDA or equivalent terms and conditions agreed.

(ii) Data Users must abide by applicable laws and University statutes, regulations and policies with respect to the use of University Data. In particular, Data Users may not use, copy, publish, store or transmit University Data in violation of copyright laws.

(iii) Data Users must respect the confidentiality of individuals, whose Personal Data they are authorised to access, and abide by the PDPA.

(iv) The University forbids the access or use of University Data by Data Users for personal gain or profit, or to satisfy personal curiosity.

(v) Data Users must comply with all applicable protection, disclosure and control procedures for University Data to which they have been granted the right to view, copy, download or otherwise access or use.

APPENDIX C: DATA CLASSIFICATION

This Appendix provides:

(i) Principles of data classification.

(ii) Pre-defined non-exhaustive list of key data sets that constitutes University Data, and the classification.

It is intended to serve as a guide to assist both Data Users and Data Stewards in the proper classification and labelling of various types of University Data using one of the classifications defined in this Policy.

The pre-defined list may be amended, modified or supplemented from time to time as is necessary to reflect any new data sets, or changes to existing data sets that the University collects, creates or otherwise handles as part of University Data.

1. Classification of University Data

1.1 Once any University Data is created or collected, the relevant Data Steward must classify the data or information as soon as reasonably possible.

1.2 If data is received from another department within NUS, the Data Steward recipient must ensure his/her department handles the data according to the classification by the Data Steward disclosing the data.

1.3 If data is received from External Parties, the Data Steward must ensure his/her department classifies the data to govern the use, storage, and management of the data according to the terms and conditions of the agreement with the External Parties.

Considerations when classifying data:

1.4 In assigning a classification to University Data under their functional areas, Data Stewards should consider:

(i) Whether there is any pre-defined classification for the relevant data set

(ii) The impact on the University or the person to which the data relates in the event:

- of unauthorised or unintentional disclosure
- the data is incomplete, inaccurate, modified unintentionally or without authority
- the data is inaccessible or destroyed unintentionally or without authority
- extensiveness or significant number of records to be shared or released to External Parties

(iii) Whether there are any contractual or statutory obligations requiring the University to:

- ensure the confidentiality of the data
- maintain the accuracy or completeness of the data
- ensure the data is readily accessible and available

(iv) Applying a minimum classification of "NUS Restricted" if it is not clear that the University Data should be considered "Unclassified".

(v) Exercising discretion when considering impact to University operations.

2. Implications of Classification

The classification assigned to the University Data determines:

(i) Access to the data
(ii) Use of the data
(iii) Approvals required for sharing and disclosure
(iv) Security measures to be taken to protect the data

3. Compilation of University Data

Where a compilation of University Data is made up of University Data from more than one classification, that compilation of University Data must be classified according to the highest classification of the data included.

4. Escalation of Classification

Where any University Data meets any of the following criteria:

(i) where its loss or leakage, regardless of sensitivity, will have regulatory, legal or financial implications to the University or affect the reputation of the University

(ii) where the data is sensitive and can identify an individual or a group of individuals e.g. VIPs

(iii) where the volume of data, regardless of sensitivity, is relatively significant

the data classification must be escalated to NUS Confidential and treatment and protection for such data must be according to the protection measures for NUS Confidential data.

6. Pre-defined Key Data Sets

- **All Personal Data**

  (includes applicants, referrers, next-of-kin, staff, contingent (casual) staff, students, patients, alumni, donors, members (e.g. library), student helpers, volunteers, contractors, vendors, temporary workers, visitors, and any records with distinctive conditions/circumstances such that one can identify an individual even when anonymised (without name or identification number)

  Notes in relation to handling Personal Data that are used as Business Contact Information or for business use under the Personal Data Protection Act 2012 (PDPA):

  - Business Contact Information (BCI) provided for business use are not subject to Part III (General Rules with Respect to Protection of Data) and Part IV (Collection, Use and Disclosure of Personal Data) of the PDPA (e.g. contact details of staff and vendors for official use including name, organisation/department, designation, office contact numbers and email).
  - Staff are deemed to have given consent for NUS to use their personal data for business purposes (e.g. managing an employment relationship).

- **Admission Data**
- **Alumni Data**
- **Donation Data**
- **Financial Data**
- **Investment Data**
- **Medical/Patient Data**
- **Research Data**
- **Staff Employment Data**
- **Student Data**
- **Other Documents, Information or Materials (contractual or statutory obligation)**

List of Pre-defined Key Data Sets by Data Classification

Key Data Set **Data Classification: NUS Confidential**	**Data Steward/HOD (Master Source)**
(i) All Personal Data *(excluding BCI)* *Examples:* *Personal particulars (such as Name, NRIC/Passport/FIN/Employment pass/Work Permit number, Birthdate, Race/Ethnicity, Religion, Nationality/Citizenship, Photograph, Contact details (personal non-corporate addresses/phone numbers/email addresses), Next-of-kin details, unique identifiers such as User IDs/Accounts, Staff number, Student number, Applicant/member number, etc* Exceptions: • NUS User IDs/Accounts used to control access to systems or as part of business email for contact purposes (BCI) are not NUS Confidential unless in the context when used together with the password and 2FA access • Numbers assigned by NUS for NUS purposes (e.g. Staff number, Student number, Applicant number) on their own are not NUS Confidential unless they can identify individuals in context with other data	Respective Data Steward of units capturing the Personal Data Faculties/Departments capturing own data *(e.g. hired personnel not on NUS payroll, Event participants, visitors and guests, the public for teaching & research)*
(ii) Admission Data *Examples:* *Undergraduate/Postgraduate Admission data (Academic qualifications , Test scores (GMAT/ GRE/IELTS/SATS/TOEFL), Referee Reports, Declarations (special needs, criminal offences), Admission Points, Comments and Outcome), etc.*	Office of Admissions (OAM)/Schools or Faculties/Programmes with own admission data *(e.g. Yale-NUS College, Asia Research Institute (ARI), Asian Graduate Student Fellowships)*
(iii) Alumni Data *Examples:* *Personal particulars, employment details, education history/records, etc.*	Office of Alumni Relations (OAR)/Faculty/Department capturing own data

Key Data Set **Data Classification: NUS Confidential**	**Data Steward/HOD (Master Source)**
(iv) Donation Data *Examples:* *Monetary Donations and Gifts-in-kind with instructions for liquidation (e.g. artefacts, land and buildings) and/or Gift Purpose as well as any relating to Anonymity of donor or gift with respect to public recognition, etc.*	Development Office (DVO)/Faculty/Department capturing own data *(e.g. Faculty/ Department, NUSSU/Sports club/ Student-led fundraising activities, partnership with external organisations where NUS is the beneficiary)*
(v) Financial Data *Examples:* *Salary/Payroll, Bank account information of Staff, Students and Visitors, All Credit card information, Donation records and tax deduction receipts, Information relating to loss/damage of assets (Fraudulent), etc.*	Office of Finance (OFN)
(vi) Investment Data *Examples:* Information on Potential investments or investment managers with Confidentiality Undertaking, etc.	Investment Office (IVO)
(vii) Medical/Patient Data *Examples:* *Medical and Counselling related information, Medical Conditions, Case History, Diagnosis, and Case Note, etc.*	University Health Centre (UHC)/Teaching & Research units
(viii) Research Data *All Research information of Intellectual Property* *Examples:* *Raw/Processed/Analysis Data, Ethics applications and related documentation which would include consent forms, information provided by/to Government Ministries and Agencies, Methodologies and Workflows, Protein or Genetic Sequences, Test Results and Responses, Questionnaires, Software programs, Algorithms, etc.*	Office of the Deputy President (Research and Technology)(ODPRT)/Faculty/Department capturing own research data

Key Data Set **Data Classification: NUS Confidential**	**Data Steward/HOD (Master Source)**
(ix) <u>Staff Employment Data</u> *Examples:* *Job Application details of Staff for Internal transfers, etc., Salary (including Base Salaries, Bonuses, Employers' CPF contributions and Other Payments made to staff), Appraisal (including Gradings, Comments and Recommendations (on promotions, re-appointments, salary adjustments and bonuses)*	Office of Human Resources (OHR)
(x) <u>Student Data</u> *Examples:* *Examination Papers, Marks/Grades, SAP/CAP, Test Scores (TOEFL/GRE/QET/DET), Special Needs-related (medical or physical disability conditions), Offences-related, etc.*	Registrar's Office
(xi) <u>Other documents, information or materials</u> which NUS has contractual or statutory obligation to protect and keep confidential *Examples:* *Senate/UCEP/BUS/BGS Minutes and Circulars, Committee of Inquiry (COI) reports, Data Leakage Incident Reports (involving NUS Confidential/ Personal data), etc.*	Respective Faculty/ Department

Key Data Set **Data Classification: NUS Restricted**	**Data Steward/HOD (Master Data Source)**
(i) Business Contact Information (BCI) *Examples:* *Information on business cards such as name, designation/title, contact numbers and address, skype and email including those of NUS staff*	Respective Faculty/Department
(ii) Employment Data *Examples:* Current/ex-Staff /Alumni employment details that are aggregated, banded and/or de-identified salary information of alumni and graduates, *leave and training records, qualifications, etc.*	OHR/OAR/Faculty/ Department
(iii) Financial Data *Examples:* Operating Budget and Ancillary Funds for the University, Annual Sinking Fund, Debt borrowings under the Debt-Grant Framework, Central Reserves, Non-fraudulent information of loss/damage of assets, Restricted Financial records (e.g. management accounting info.), Vendors' bank account details, etc.	OFN
(iv) Investment Data *Examples:* Internal investment proposals and reviews, (e.g. investment managers' performance), financial and non-financial investment reports	IVO
(v) Research Data *(excludes those that involve Intellectual Property)* *Examples:* *Raw data, Processed data, Analysis data, Ethics, Applications and related Documentation (including consent forms, grants and grant related data such as proposals from PIs), Information provided by/to Government ministries and agencies, Publication, In development information (doesn't contain IP or Trade Secret), Research Collaborations and related documents, Published Output, Questionnaires Drafts of scientific papers*	ODPRT/Faculty/Department capturing own data

Key Data Set **Data Classification: NUS Restricted**	**Data Steward/HOD (Master Data Source)**
(vi) <u>Student Data</u> *Examples:* *Academic degree programmes, study abroad programmes, internship, work attachments/ experience, CCA-related including Qualifications, Work Experience, Service Indicators/Holds, Leave of Absence, Graduate & Undergraduate Financial Aid data, Scholarship data*	Registrar's Office
(vii) <u>Internal Policies, Procedures and Circulars</u> *Examples:* *Messages from management to faculty and staff*	Respective Faculty/Department

Key Data Set **Data Classification: Unclassified**	**Data Steward/HOD** **(Master Data Source)**
General Communication and Publicity *Examples:* *General circulars or emails, publicly posted press releases, University maps, newsletters, newspapers and magazines*	Respective Faculty/ Department

APPENDIX D: DATA COLLECTION AND STORAGE

This Appendix provides:

(i) Some considerations when collecting and storing University Data:

- from NUS Staff, Non-NUS Staff and External Parties
- in University systems and non-University systems
- on the internet

(ii) Other considerations

1. NUS Staff, Non-NUS Staff and External Parties

1.1 It is vital to safeguard University Data at all times when collecting or storing data from NUS Staff, Non-NUS Staff and External Parties.

1.2 Examples of External Parties include NUS/non-NUS students (and their family members), alumni, family members of staff, ex-staff, donors, government agencies, other academic/research institutions, external organisations and any other person who is not a Data User.

1.3 Data collected from External Parties and stored by NUS must only be for NUS business purposes. The data must be anonymised if the purposes do not need to identify the individual (e.g. patient data used for research).

1.4 Regardless of the party involved, please ensure that University Data is secure when considering how the data is collected and where the data is stored.

2. University Systems and Non-University Systems

2.1 University Data must be securely collected or disclosed, and kept secure at all times when stored in both University systems and non-University systems such as External Party's or service provider's systems or cloud services.

2.2 Non-University systems can also refer to situations when Data Users do work using computers, notebooks or devices available that were not issued by the University (e.g. at home or personally-owned). Data Users who choose to use such non-University systems for work are responsible for ensuring the security of the University Data stored in these systems and they must not put University Data at risk.

2.3 All NUS Confidential University Data and NUS Restricted Administrative Data to be stored on servers or storage systems, must only use servers or storage either of University systems or non-University systems covered by an agreement with the University (e.g. enterprise-subscribed cloud services).

3. Internet

Any transmission of NUS Confidential data over the internet must be in encrypted format.

4. Other Considerations

Data Stewards, with assistance from appointed Data Managers, must review data collected and stored, ensuring as far as possible that:

(i) the data is safeguarded and kept secure by using the data protection measures in this DMP or equivalent measures;

(ii) no item is collected twice from the same department or individual, unless at the time of collection, the data could not be obtained from another source in a timely and cost-effective manner;

(iii) minimal data is collected for the specified purpose, that is, avoid collecting data unnecessarily or excessively; and

(iv) due diligence is done to comply with the PDPA Compliance Guidelines when collecting Personal Data such as ensuring notification and consent is obtained prior to collection (e.g. use of the NUS Personal Data Notice for Student Applicants when collecting personal data from prospective students).

APPENDIX E: DATA SHARING AND DISCLOSURE

This Appendix provides:

(i) Review and approval processes for data sharing with Data Users within NUS and data disclosure to External Parties.

(ii) Protection measures and documents required for releasing of data when approved.

It is intended to serve as a guide to assist both Data Stewards and Data Users to ensure proper review and approval has been given prior to data sharing or data disclosure.

Exceptions from having to seek approval

(i) When data is requested from law enforcement agencies (e.g. Singapore Police Force, Criminal Investigation Department, Corrupt Practices Investigation Bureau); or

(ii) In the case of emergencies involving life and death.

1. Data Sharing with Data Users within NUS

(Sharing of University Data with those who do work for NUS)

1.1 Data sharing refers to the sharing of University Data with Data Users.

1.2 The following summarises the process and requirements for sharing data with Data Users and highlights cases where exceptions apply.

(i) Data Users requiring access to University Data must request for the data/approval from the respective Data Stewards/Data Managers who will review the request according to the purposes required.

(ii) Refer to **Appendix C** for the List of Pre-defined Key Data Sets and respective Data Stewards.

(iii) Data Stewards/Data Managers approving data requests (e.g. Office of Human Resources for Staff data, Registrar's Office for Student data) are to share data or grant access to data according to the following:

- Ensure that data is given as needed for its intended purposes, and for the business or in the interest of the University.
- Ensure that data is used only for the purpose of collection within the Data Users' scope of work and duties as defined by the Data Stewards.
- In the course of conducting University related business or matters with External Parties, ensure that data is used in accordance with the terms and conditions of the agreement signed with External Parties (e.g. data received by the University from organisations or government ministries/agencies)

- Ensure that consent has been given by individuals (for Personal Data).

- If data access is given to Non-NUS Staff to do work for NUS, ensure that they are bound by an NDA or equivalent prior to disclosure.

  Important when sharing with Non-NUS Staff:

  For highly sensitive NUS Confidential data (e.g. Medical/Patient, Donor, VIPs), Data Stewards must also seek approval from the relevant member of Senior Management (* see NUS Management below) with responsibility over the functions from where the data was requested.

  * NUS Management refers to NUS leadership team led by NUS President. If the member of NUS Management is also the Data Steward seeking approval, he/she should seek approval from the next higher level of authority. The NUS President has overall authority to approve all University Data disclosures.

- Ensure data definitions and business rules governing the appropriate use of the data are shared where necessary.

- Use a secure mode of transmission or access (e.g. via secure IT application systems, encrypted files or folders like nBox, or encrypted email and attachments).

(iv) Departments/Data Users must only use the data for the intended purposes as stated in their requests or as agreed with the Data Steward/Data Manager according to the following:

- Ensure secure storage of data, secure transmission of data and secure disposal of data using the data protection measures in this Policy or equivalent measures.

- Inform Data Stewards/Data Managers (of departments providing the data) when there is a change of purpose for data use.

- Inform Data Stewards/Data Managers (of departments providing the data) of any data quality issues or any misuse or data incidents (loss or leakage).

2. Data Disclosure to External Parties

(Disclosure of University Data to those who do not do work for NUS)

2.1 Data disclosure refers to the disclosing of University Data to External Parties. External Parties include NUS/non-NUS students (and their family members), alumni, family members of staff, ex-staff, donors, government agencies, other academic/research institutions, external organisations, service providers, vendors and any other person who is not a Data User.

2.2 The following summarises the process and requirements for disclosing data to External Parties and highlights cases where exceptions apply.

(Please refer to the section 2.3 for the Data Disclosure to External Parties Process Flow.)

(i) External data requests for NUS Confidential or NUS Restricted Data must be:

- reviewed and approved by the Head of Department (HOD)
- supported by the respective Data Stewards (if the HOD is not the Data Steward)
- supported by the Data Protection Officer (for Personal Data other than Business Contact Information)

  Note: DPO will support the request as long as it complies with existing laws and policies.

(ii) For NUS Confidential or Research Grant Application data, HODs must additionally seek approval from the relevant member of Senior Management (* see NUS Management as defined above) with responsibility over the functions from where the data was requested.

(iii) Standing support/approval may be obtained for similar requests that are frequent or regular.

(iv) Considerations by approving authority before approval:

- Consider whether the purpose for which disclosure is to be made is legitimate and ensure that any disclosure made does not go beyond that required to fulfil the specified purpose.
- Where applicable, ensure that an NDA (or equivalent terms and conditions) requiring the External Party to maintain confidentiality is in place prior to Data Disclosure.
- Ensure that the disclosure will not contravene or violate any law, the provisions of any applicable agreement, this DMP or any other applicable policy, procedure or document.

(v) Requester or requesting department must:

- Ensure that data retention policies are made known to the External Parties for the data disclosed, where applicable
- Ensure data is disclosed in a secure manner using the data protection measures in this Policy or equivalent measures
- Ensure Non-Disclosure Agreement (NDA) is signed (or is otherwise in place) before disclosing data to External Parties

  Exceptions:

(a) Confidentiality Undertaking (CU) with acknowledgement (for purposes of seeking support/funding from non-government agencies)
(b) Confidentiality Undertaking (CU) without acknowledgement (for Government agencies)
(c) NDA/CU not required (if required by law or submission is online via government websites)

For all cases – Standard Non-Disclosure Agreement (NDA)

When disclosing data, use the standard NDA (except in relation to research collaboration related activities). Where it is necessary to revise the standard NDA to suit individual circumstances, department/unit should consult with the Office of Legal Affairs.

For research collaboration related activities, please refer to the Research Data Management Policy. Please request for the research NDA form from the OFFICE OF THE DEPUTY PRESIDENT (RESEARCH AND TECHNOLOGY), INDUSTRY ENGAGEMENTS & PARTNERSHIPS.

Please refer to Sections 10.2 and 10.3 of the Policy on Approving and Signing Authority on approvals and authorised signatories for NDA.

For exception cases only – Standard Confidentiality Undertaking (CU)

(a) Standard Confidentiality Undertaking where acknowledgement is required from external party – *To be used **ONLY** for cases where NUS is receiving funding/support from external party and external party is a non-government agency*

"With reference to your request for information relating to National University of Singapore (NUS) (defined as "University Data"), please be informed that the University Data may be disclosed in writing or verbally to you. In compliance with NUS' internal policies, we request that you hold and keep the University Data in strictest confidence and not divulge it to any third party. Please ensure the security and control of the University Data and that it would not be copied or reproduced in any form or used beyond the purpose envisaged, without NUS' prior written authorisation. Please promptly return or destroy the University Data, if requested by NUS.

We would be grateful if you could confirm your acknowledgement and agreement to the above confidentiality obligations in writing, either by reply email or letter, before we furnish the University Data to you."

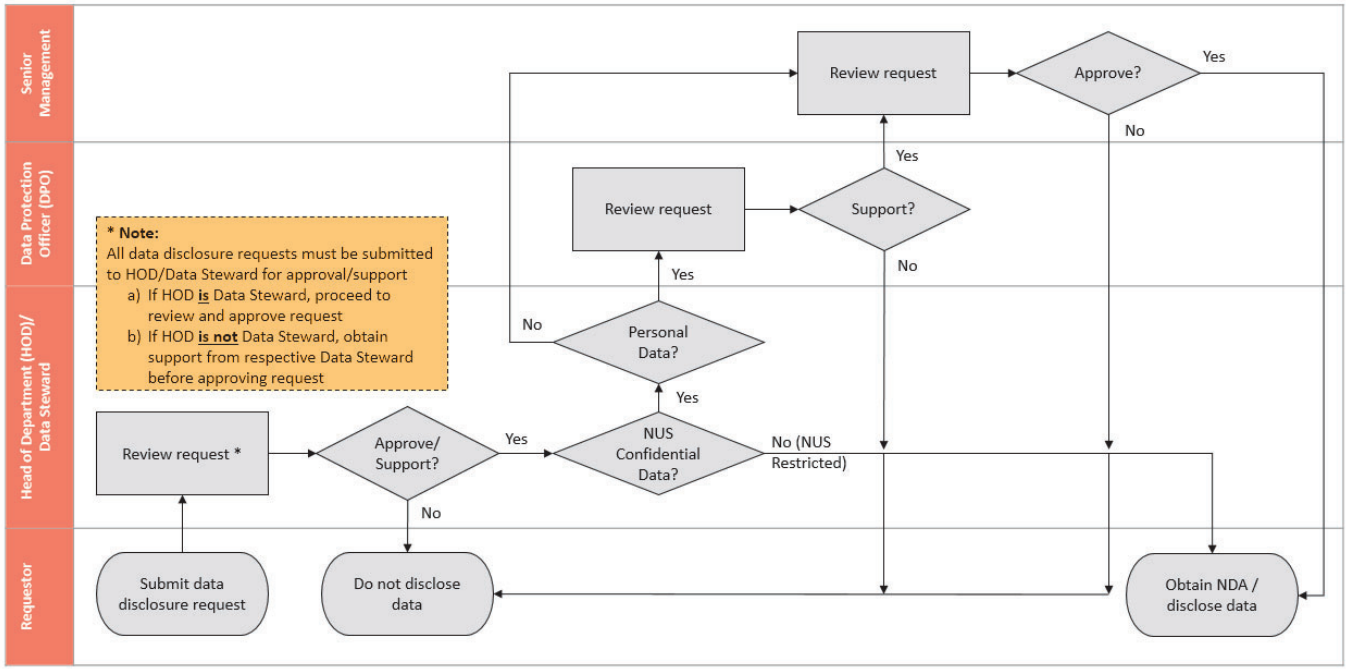
(b) Standard Confidentiality Undertaking where no acknowledgement is required from external party – *To be used **ONLY** for cases where external party is a government agency*

"With reference to your request for information relating to National University of Singapore (NUS) (defined as "University Data"), please be informed that the University Data may be disclosed in writing or verbally to you. In compliance with NUS' internal policies, we request that you hold and keep the University Data in strictest confidence and not divulge it to any third party. Please ensure the security and control of the University Data and that it would not be copied or reproduced in any form or used beyond the purpose envisaged, without NUS' prior written authorisation. Please promptly return or destroy the University Data, if requested by NUS.

Your receipt and use of the University Data would be deemed as your confirmation and agreement to the above confidentiality obligations."

2. DATA DISCLOSURE TO EXTERNAL PARTIES

2.3. PROCESS FLOW



APPENDIX F: DATA RETENTION AND DISPOSAL

This Appendix provides:

(i) Considerations for data retention and some retention policies.

(ii) Considerations for data disposal.

1. Data Retention

1.1 Data Stewards/Data Managers are responsible for the retention and archival of University Data within their functional areas taking into account the following considerations:

(i) Legal Requirements

Data Stewards must consider whether there are any legal requirements regarding the retention of University Data within their functional areas.

For example, the period for retention of accounting records under the Companies Act (Cap. 50) is at least 5 years from the end of the financial year in which the transactions or operations to which those records relate are completed.

For University Data that includes Personal Data, Data Stewards must ensure that the University complies with the retention limitation obligations under the PDPA. Refer to the PDPA Compliance Guidelines for details.

(ii) Business Requirements

Data Stewards must consider what University Data would need to be retained to sufficiently maintain administrative operations, comply with contractual obligations, remain accountable to the stakeholders of the University and meet other business requirements.

(iii) Historical Significance to NUS

Data Stewards should consider what items or categories of University Data contribute to the history of NUS.

1.2 The following are some retention policies on NUS Student and NUS Staff data, developed by the respective Data Stewards, which can be found in the Staff Portal under Policies:

(i) Retention and Archival of Student Academic and Curriculum Records
(ii) Retention and Archival of Examination-related Records
(iii) Retention Policy for Personal Data of Staff

1.3 Where there is a need to retain Personal Data for purposes other than legal or business, consider anonymising Personal Data by removing identifying information such that the remaining data does not identify any particular individual.

1.4 Data Stewards/Data Managers should consider making known the data retention policies when disclosing data to External Parties where applicable.

2. Data Disposal

2.1 When University Data is no longer required for purposes such as those stated above, Data Stewards must ensure the University ceases to retain the data.

2.2 The data must be disposed of in a secure manner such that the disposed data cannot be retrieved in the process of disposal or cannot be recovered after it is disposed of. This can be done through a trusted party or using a reliable and secure system/technology.

Disposing Data in Storage Media

The following are considerations to dispose University Data in storage media:

(i) Erase and destroy all University Data in storage media before disposing or redeploying the media (e.g. using Blancco).
(ii) Physically destroy any functional or non-functional storage media for situations where the data cannot be securely erased. Shred or incinerate Solid State Drives (SSD) and degauss Hard Disk Drives (HDD).

Data Users Who No Longer Work for NUS

Data Users upon leaving the service of the University or no longer do work for the University must ensure they do not retain any University Data that should not be in their possession. If in doubt, they should consult the Data Stewards prior to their departure. They must:

(i) Ensure any Master Source data that should no longer be in their possession is handed over to those appointed to take over responsibility for the data.

(ii) Securely remove all electronic data that should no longer be in their possession from storage media, computers, notebooks and devices not issued by the University (e.g. those that are personally-owned).

(iii) Shred or incinerate all non-electronic (hardcopy) data that should no longer be in their possession and are no longer required by the University.

APPENDIX G: DATA PROTECTION

This Appendix provides:

(i) Considerations to protect data and mitigate the risks of data loss or leakage.

(ii) Anonymisation of Personal Data.

(iii) Measures to protect data (electronic and non-electronic).

1. Considerations to Protect Data

To mitigate the risks of data loss or leakage, Data Stewards/Data Managers/Data Users should consider using the following:

(i) Have process controls and checks to help identify or mitigate the risk of human error when handling data.

(ii) Implement standard operating procedures (or SOPs) to be followed so necessary steps to protect data are carried out.

(iii) Anonymise Personal Data so the data cannot identify or relate to any individual.

(iv) Use technology and tools (e.g. encryption, firewalls, access controls and monitoring) to help protect data in storage and transmission.

(v) Conduct training for new Data Users and refresher training to remind existing Data Users of the best practices to protect data.

2. Anonymising Personal Data

2.1 Anonymisation 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.

When to Consider Anonymisation?

2.2 It is good practice prior to collection, use or disclosure of Personal Data, for Data Stewards to consider whether individuals need to be identifiable throughout the period their data is kept. Before any use or disclosure, Data Stewards should consider anonymisation if use of personally identifiable information is not required (e.g. patient data used for research).

2.3 Data Stewards should consider anonymisation (instead of data destruction) when the work is completed, all purposes have been fulfilled, and only if retaining such anonymised data is beneficial to the University. This may include compiling historical statistics or performing data analytics. Data anonymisation will enable the University to comply with its PDPA obligation when it is no longer necessary to retain Personal Data for legal or business purposes.

2.4 For information on the different techniques of anonymisation, please refer to the Personal Data Protection Commission (PDPC) website and the PDPC's "Guide to Basic Data Anonymization Techniques".

Re-identification

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

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

3. Measures to Protect University Data

3.1 The following best practices must be read in conjunction with related policies including PDPA Compliance Guidelines, IT Security Policy, Acceptable Use Policy, Guidelines for Acceptable Use and Cloud Policy.

3.2 To protect the confidentiality and integrity of University Data, consider applying the protection measures for:

(i) Data at endpoint – data which resides in PCs, notebooks, mobile devices and storage devices.
(ii) Data in motion – data which traverses across the network or is transported between sites.
(iii) Data at rest – data in servers, databases, backup media and storage platforms including those on premises and in the cloud.
(iv) Data in hard copy – data in the form of printed paper or non-electronic versions.

3.3 Some considerations for the selection of protection measures include:

(i) Sensitivity of data by itself, with or without contextual information
(ii) Whether data is for internal or external consumption
(iii) Impact vs likelihood of data leakage
(iv) When data is transmitted or stored outside secure storage such as nBox (encrypted by default)

3.4 If it is not possible to implement the measures in the DMP Data Users must consult with Data Stewards before adopting equivalent protection measures to ensure that the alternative measures are adequate. Data Stewards should consult with NUS IT if in doubt.

APPENDIX H: DATA INCIDENT REPORTING

This Appendix provides:

(i) Considerations to determine data loss or leakage.

(ii) Process for reporting data incidents.

(iii) Template for reporting data incidents.

1. Considerations to Determine Data Loss or Data Leakage

1.1 Data Loss occurs when University Data:

(i) is completely lost;
(ii) is no longer accessible;
(iii) cannot be recovered or retrieved from backup sources; or
(iv) cannot be recreated as no other copies or documentation exist.

1.2 Data Leakage occurs when University Data is intentionally or unintentionally:

(i) accessed by unauthorised parties; or
(ii) made available to unauthorised parties.

2. Process for Reporting Data Incidents

Data Users or Departments who are involved in or aware of data loss or leakage must report the incident immediately according to the following process:

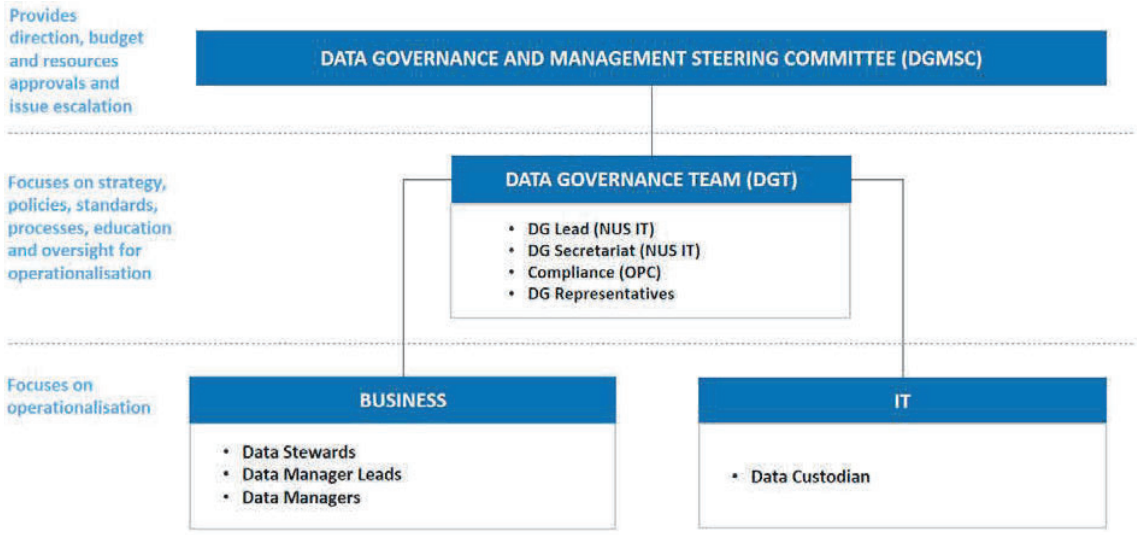
(i) Reporting personnel (involved or aware) to report the incident to the Head of Department using the Data Incident Report template (**Appendix H-1**).
(ii) Head of Department will review the incident to assess the risk, impact, corrective and preventive actions taken or to be taken, and adequacy of controls.
(iii) If the Head of Department is not the Data Steward, he/she must inform the Data Steward who will also review the incident.
(iv) If the incident involves Personal Data, he/she must also inform the Data Protection Office (DPO) through the Office of Privacy and Compliance (OPC) to review the incident.
(v) The final data incident report must be sent by the reporting personnel's department to NUS IT (dmp@nus.edu.sg) for reporting to the Risk Management Steering Committee (RMSC) through the Office of Risk Management (ORM).
(vi) ORM will inform Data Stewards/Departments and NUS IT of the outcome of any decisions made at RMSC.

APPENDIX H-1 : DATA INCIDENT REPORTING

3. Template for Reporting Data Incidents

The template can be accessed from Staff Portal under Information Technology, IT Security Portal, Loss or Leakage of University Data Reporting.

APPENDIX I: DATA GOVERNANCE OPERATING MODEL



Key Roles in Data Governance

1. Data Governance Lead (DG Lead)

1.1 The DG Lead is responsible for defining the enterprise data governance strategy and goals, and champion all data governance initiatives towards achieving these goals.

1.2 The DG Lead key responsibilities are:

(i) Define enterprise data management strategy

- Set clear direction, objectives and targets for the DGT, ensuring they are aligned with NUS' strategic priorities

(ii) Champion data management initiatives across the enterprise

- Facilitate the identification of specific initiatives required to meet DGT's goals
- Work closely with business and IT to drive these initiatives
- Obtain Data Governance and Management Steering Committee (DGMSC) support for specific initiatives
- Represent the DGT in DGMSC meetings

(iii) Accountable for program budget

- Develop and obtain approval for data governance budget
- Monitor and manage data governance budget

(iv) Resolve data related issues/risks

- Decide solution for data issues/risks

- Keep stakeholders informed of progress and potential impact of issues/risks identified
- Seek guidance from DGMSC for issues/risks that need to be escalated

(v) Engage DGMSC for awareness campaigns

- Get buy-in and engage DGMSC to champion cultural awareness activities
- Monitor the communication and training plan

2. Data Governance Secretariat (DG Secretariat)

2.1 The DG Secretariat is responsible to facilitate and support NUS' data governance administrative matters.

2.2 The DG Secretariat key responsibilities are:

(i) Manage communication between DGMSC and stakeholders
(ii) Ensure proper logistics for Data Governance initiatives and activities
(iii) Prepare qualitative agendas and minutes for the DGMSC
(iv) Maintain relevant records of DGMSC decisions

3. Data Governance Representatives (DG Representatives)

3.1 Data Governance Representatives are appointed by DGMSC members to be core members of the DGT who focus on strategy, policies, guidelines and processes, as well as education and oversight for overall DG operationalisation.

3.2 The DG Representative key responsibilities are:

(i) Work closely with the DG Lead to drive data management initiatives across the enterprise

- Define and review DG policies, guidelines and processes
- Drive adoption of DG processes and policies within their respective cluster and departments

(ii) Manage communication for processes and policies within their respective cluster and departments

- Communicate new and changed processes and policies to those who may be impacted

(iii) Resolve data related issues/risks

- Provide solutions for data issues/risks

4. Data Manager Leads (DM Leads)

4.1 Data Managers Leads are appointed by the Data Steward to lead data management activities in their department. The Data Steward will appoint from the appointed

Data Managers in their department, two members to be DM Leads. These DM Leads will work with their respective DG Representative in the DGT.

4.2 The DM Lead key responsibilities are:

(i) Work closely with the DG Representative to drive data management initiatives across the department

- Drive adoption of DG processes and policies within their department

(ii) Manage communication for processes and policies within their department

- Communicate new and changed processes and policies to those who may be impacted

(iii) Resolve data related issues/risks within their department

- Provide solutions for data issues/risks

~ End of Appendices ~