NUS DATA MANAGEMENT POLICY

Policy Information	
Category	Governance/Administrative/Operational
Department Responsible	NUS Information Technology (NUS IT)
Contact	Email: dmp@nus.edu.sg
Governance (approved by)	Data Governance and Management Steering Committee (DGMSC)
Audience (applies to)	All users of University Data including: • NUS Faculty and Staff • Part-time Teaching Staff • Contingent (casual/temporary) Staff • NUS and Non-NUS Student assistants, interns, helpers or volunteers (e.g. in departments, NUSSU, clubs and societies, halls and residences) • Volunteers • Contractors, vendors, temporary workers
Brief Purpose	Defines general principles to govern the appropriate collection, use, maintenance, disclosure, disposal and protection of University Data
Initial Version	Version 1.6 – 15 May 2007
Current Version	Version 3.0 – 1 May 2020

Contents

1. PURPOSE

1.1 The NUS Data Management Policy ("DMP") governs the collection, use, maintenance, disclosure, disposal and protection of University Data and defines the general principles to safeguard University Data.

The six general principles are:

(i) Shared Responsibility through Data Stewardship and Usage
(ii) Confidentiality through Data Classification
(iii) Single Source of Truth through Data Collection and Storage
(iv) Need To Know through Data Sharing and Disclosure
(v) Need To Keep through Data Retention and Disposal
(vi) Security through Data Protection

1.2 Users must adhere to the DMP and use University Data only for the University's purposes to advance its interests. A secure, reliable and accessible University Data source is a valuable asset that will enable the University to make effective decisions to meet the University's education and research objectives as well as comply with the law.

1.3 The DMP serves as an overarching policy for all data management-related documents and activities in the University. As such, all data management-related policies, standards, procedures and guidelines must be aligned with the DMP.

2. DEFINITIONS AND SCOPE

2.1 Please refer to **Appendix A** for all Definitions referenced in this DMP.

2.2 University Data refers to 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.

University Data 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.

2.3 Users should refer to the following specific policies and guidelines governing various types of data or consult with the respective offices for any enquiries.

Data Type	Policy	Contact
Administrative Data	This DMP	NUS IT DMP Team at dmp@nus.edu.sg
Research Data	Research Data Management Policy RDMP Guidelines	Office of the Deputy President (Research and Technology) at rcio@nus.edu.sg
Personal Data	NUS Personal Data Protection Policy NUS PDPA Compliance Guidelines	Data Protection Officer (DPO) at dpo@nus.edu.sg
Teaching and Instructional Materials	-	Office of the Senior Deputy President and Provost

2.4 A Data User is any person who has access to University Data to do work for NUS. Data Users include all NUS Staff and Non-NUS Staff. They do not include External Parties who do not do any work for NUS. Data Users have shared responsibility to ensure the appropriate use, integrity, classification and protection, of University Data. Although they have access to the data, they may only share with or disclose to others based on proper authorisation. When in doubt, they take guidance from respective Data Stewards in the handling of University Data.

2.5 The DMP applies to all Data Users who have access to University Data. Data Users include:

NUS Staff

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

Non-NUS Staff

(iv) NUS and Non-NUS Student assistants, interns, helpers or volunteers (e.g. 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

2.6 Data Users do not include those who are "customers" of the University (e.g. applicants and students in general) as they typically only access their own data for their own purposes. As such, the DMP does not apply to them.

3. SHARED RESPONSIBILITY: DATA STEWARDSHIP AND USAGE

3.1 The principle of Shared Responsibility requires that all Data Users share the stewardship responsibility to use, accurately present and protect the data as a valuable asset of the University.

3.2 Use of University Data is solely for the conduct of University business, including analytics and research authorised by the University.

3.3 The University is the Data Owner of all University Data. This means University Data belongs to the University and does not belong to any individual or department.

3.4 Individual departments have stewardship responsibilities on behalf of the University. The department head undertakes the role of Data Steward for University Data within his/her functional area.

3.5 The Data Steward is accountable for University Data within his/her functional area and ensures the accuracy, integrity, ethical conduct and use, availability and security of the data. This includes:

(i) Defining the purpose and use of the data
(ii) Classifying the data
(iii) Creating, collecting and updating the data
(iv) Controlling access to the data
(v) Archiving or disposing the data
(vi) Ensuring the security of the data

3.6 Please refer to **Appendix B** for more information on Data Stewardship and Usage Roles and Responsibilities.

4. CONFIDENTIALITY: DATA CLASSIFICATION

4.1. The principle of Confidentiality necessitates that University Data must be handled and protected based on its level of sensitivity or classification.

4.2. The University has classified University Data as follows:

(i) NUS Confidential applies to data, information, documents or materials that are sensitive or critical, including Personal Data and proprietary information, for use by authorised users in their work or duties.

Loss or leakage will likely have *regulatory, legal or financial implications* to the University or *damage the reputation* of the University.

(ii) NUS Restricted applies to data, information, documents or materials (other than those classified as NUS Confidential) that are for use by authorised users in their work or duties.

Loss or leakage will likely *cause some embarrassment* to the University.

(iii) Unclassified applies to data, information, documents or materials (other than those classified as NUS Confidential or NUS Restricted) that may not be restricted to authorised users and may be released to students in general or the public.

Loss or leakage will likely *have minimal impact* to the University.

4.3. These classifications will determine the handling of University Data in terms of collection, access, use, maintenance, protection, disclosure, retention and disposal.

4.4. Data Users are required to label documents or materials containing University Data according to the classifications determined by respective Data Stewards or as documented in this DMP.

4.5. University Data should be classified as NUS Restricted at the minimum when the classification of any data remains in doubt upon consultation with the Data Steward.

4.6. Any data, information, documents or materials with no classification (or not labelled) will be treated as Unclassified.

4.7. Data Stewards and Data Users must always be mindful of the consequences to the University should any data, information, documents or materials be classified inappropriately.

4.8. Please refer to **Appendix C** for more information on Data Classification.

5. SINGLE SOURCE OF TRUTH: DATA COLLECTION AND STORAGE

5.1 The principle of the Single Source of Truth calls for consistently preserving the quality of a Master Source of University Data across the University.

5.2 To uphold this principle, departments must not create, collect or duplicate key data sets, as defined by the Data Governance Team, which have already been created or collected as a Master Source (such as personal data and administration data). They should instead request for access to the Master Source data from the relevant departments.

5.3 When engaging with an External Party, Data Stewards and Data Users must only use confidential data disclosed by the External Party for the intended purposes of the engagement and protect it according to the agreed terms and conditions. If both parties have yet not finalised the confidentiality terms and conditions prior to receipt of such confidential data, then Data Stewards and Data Users must apply the same confidentiality standards and protection that the University uses to safeguard NUS Confidential University Data. Data Stewards and Data Users must not share such confidential data with any other External Parties without the explicit consent of that originator External Party.

5.4 Data Stewards and Data Users are to create, collect, maintain and store University Data in a secure manner using the data protection measures specified in this DMP to safeguard and ensure accuracy and quality of the data.

5.5 Please refer to **Appendix D** for more information on Data Collection and Storage.

6. NEED TO KNOW: DATA SHARING AND DISCLOSURE

6.1 The principle of Need to Know establishes that access to University Data is given as needed for its intended purposes to advance the interest of the University.

6.2 Data Users who share University Data (classified as NUS Confidential or NUS Restricted) with other Data Users within or across departments must ensure they do so with proper authorisation from the respective Data Stewards or Data Managers. In addition, please note that the Data Steward role is not transferred to the receiving party when University Data is shared within or across departments.

6.3 Departments are to share University Data with other departments upon their reasonable requests so that they derive data from a consistent single source of truth and Master Source that is reliable. Departments with access to the shared data must also ensure the shared data remains the Master Source and avoid creating a duplicate data source.

6.4 When disclosing University Data (classified as NUS Confidential or NUS Restricted) to External Parties, Data Stewards and Data Users must comply with the data disclosure approval processes defined in the DMP.

6.5 When sharing or disclosing University Data, Data Stewards and Data Users are to ensure that it is done in a secure manner using the data protection measures in this DMP.

6.6 Refer to **Appendix E** for more information on Data Sharing and Disclosure.

7. NEED TO KEEP: DATA RETENTION AND DISPOSAL

7.1 The principle of Need to Keep highlights to the Data Stewards and Data Users that they should not retain University Data for longer than necessary or in perpetuity.

7.2 Data Stewards and Data Users are to ensure University Data is stored only for as long as required, regardless of where the data may be present or stored.

7.3 Where there is no longer a legal or business reason to store certain University Data, it must be disposed properly using secure data disposal measures in this DMP.

7.4 Please refer to **Appendix F** for more information on Data Retention and Disposal.

8. SECURITY: DATA PROTECTION

8.1 The principle of Security recognizes that University Data is a valuable asset and mandates that it must be safeguarded and kept secure from unauthorised access or inappropriate use.

8.2 Data Stewards and Data Users must protect University Data at all times. They must perform checks and due diligence through various ways including the use of process controls and checks, standard operating procedures, anonymisation, technology and tools, as well as education.

8.3 As a best practice, University Data in electronic form and classified as NUS Confidential must be protected using encryption.

8.4 University Data in non-electronic form (hardcopy) and classified as NUS Confidential must be locked when not in use and must not be left unattended during use.

8.5 Please refer to **Appendix G** for more information on Data Protection.

9. DATA INCIDENT REPORTING

9.1 Data Users who become aware of any loss or leakage of University Data classified as NUS Confidential or NUS Restricted data must immediately report the incident to the respective Head of Department. The Head of Department must report the incident to NUS IT.

9.2 For data incidents involving Personal Data, the Head of Department must also report the incident to the Data Protection Officer immediately.

9.3 Heads of Department/Data Stewards and Data Users must comply with the data incident reporting process in the DMP. Please refer to **Appendix H** and **Appendix H-1** for the Data Incident Reporting process and template respectively.

10. GOVERNANCE AND REVIEW

10.1 The Data Governance and Management Steering Committee (DGMSC) provides overall oversight and guidance to all matters relating to this DMP. The DGMSC is an executive forum that oversees data governance and strategic development as well as addresses resourcing and the escalation of issues in the management of University Data.

10.2 DGMSC approves all policies for the management of University Data and all data management-related activities within the University.

10.3 The Data Governance Team (DGT) is a management working committee that develops the enterprise data strategy including policies, standards and processes for the appropriate management of University Data.

10.4 Data Stewards within their respective departments must ensure that the DMP and other enterprise data policies (including Research DMP) are applied and adhered to at the operational level. Data Stewards must not develop separate data policies that are not aligned with the enterprise data policies.

10.5 Please refer to **Appendix I** for the detailed Data Governance Operating Model.

10.6 The DGT will review and update this DMP from time to time as and when the need arises. Any revisions, apart from editorial changes or updates that add clarity but do not change policy positions, will be submitted by the DGT to the DGMSC for approval.

11. INTERPRETATION

In the event of any inconsistency between the requirements set out in this DMP and those set out in any other policies, standards, procedures, guidelines or other documents relating to data management and University Data, the requirements set out in this DMP will take precedence unless otherwise stated. Please consult with NUS IT for any clarification required regarding this DMP or its principles.

12. ADHERENCE

Compliance with this DMP is mandatory. The University will investigate any failure to comply with this DMP. Non-compliance includes for example, inappropriate or wrongful classification, use, sharing, storage of University Data. The University at its absolute discretion may impose corrective or disciplinary action as the University deems fit in accordance with the Staff Disciplinary Procedures and Sanctions Policy (SDP).

13. EXCEPTIONS

In the exceptional event that it is not possible or impractical to comply with any of the requirements stipulated in this DMP, the Data Steward or Data User must first consult with NUS IT to explain the situation in detail. If there is no workaround to the issue upon consultation, the Data Steward or Data User may then proceed to seek a waiver by prior written approval from the Deputy President (Administration and Finance). Such approval grant shall be at the absolute discretion of the Deputy President (Administration and Finance).

14. LIST OF APPENDICES

Ref	Appendix
A	Definitions
B	Data Stewardship and Usage Roles and Responsibilities
C	Data Classification
D	Data Collection and Storage
E	Data Sharing and Disclosure
F	Data Retention and Disposal
G	Data Protection
H	Data Incident Reporting
H-1	Data Incident Report Template
I	Data Governance Operating Model

~ End of DMP ~