UNIVERSITY OF LONDON

Data Governance Policy

(June 2022)

Version Number	Summary of Changes	Author	Date
1.0	Draft for review	Suzie Mereweather	11th February 2022
2,0	Reviewed by Jake Crittenden and Steve Terrill. Amendments incorporated	Jake Crittenden/Steve Terrill	March 2022
3.0	Additions by Jem Eskenazi		April 2022
4.0	Reviewed by Alastair Jarvis		June 2022
4.1	Final version incorporating all suggested additions and changes prepared for VCEG	Suzie Mereweather	June 2022
4.2	Final version following VCEG	Suzie Mereweather	July 2022

Document Control & Approval Process

This document was approved by VCEG on 13th July 2022

1. Introduction

1. The University operates in an increasingly complex and data-oriented environment. There is always a need for more information, insight, analysis, benchmarking and more effective business processes. Data is used in a variety of ways from primary use cases including the management of student information to secondary use cases such as the production of management information and reporting for internal key performance monitoring and external statutory returns.

2. The data generated and held by the University are key assets that must be managed correctly to underpin University strategic development, essential functions and academic integrity.

3. The University recognises the need for balance between
    - public accountability and transparency in its governance
    - compliance with regulatory obligations including data protection legislation, and
    - the need to protect the personal and commercially sensitive confidential information it holds
    - avoiding unnecessary bureaucracy.

4. A Data Governance Policy is needed to ensure that data is collected, created, managed and processed in an effective and compliant manner which
    - Meets the best interests of the University as a whole
    - Supports its organisational Strategy, and
    - Informs the design and development of its technical architecture and business processes.

2. Scope

1. This policy applies to University of London staff, students, agency staff, visitors, contractors and third parties who process University data.

2. It relates to both corporate and research data, although research data demands specialist requirements that require additional controls and governance which are not included in this document. Further policy requirements around research data are owned by the School of Advanced Studies.

3. Aims and Purpose

1. This document works alongside other University data related policies (see section 6) to effectively manage University data as an asset, supporting reliable data driven decision making from quality data sources while ensuring that data is collected, created and processed in a compliant manner in the best interests of the wider University.

2. A well-managed data infrastructure can provide the University with cost savings, new growth opportunities in student retention and can inform areas of risk and action required. To achieve robust and reliable data, requires effective governance of data sets.

3. This document therefore provides a corporate framework with defined roles and responsibilities for the collection, quality, storage, security, maintenance and dissemination of institutional data. It equips those involved with managing processes, business continuity, information compliance, business intelligence, research management/information governance and other key functions with the necessary governance to realise benefits of data management and ensure compliance.

4. This policy aims to help the University to:
   - Improve decision making from accurate and reliable data sources
   - Meet our internal and external compliance requirements, including statutory requirements such as data protection legislation
   - Reduce costs and increase effectiveness through efficient, repeatable processes and use of automation as well as storage and backup efficiency
   - Reduce risk in the management of personal data of students, staff and Alumni

4. Roles and Responsibilities

1. The University itself is the owner of all University data. No one individual, department or body owns the University's data, but specific individuals will assume roles to support effective management of that data.

2. The Pro Vice-Chancellor (Partnerships and Governance) acts as the senior University officer taking responsibility for the institution's information risk policy and approach. They ensure that information risks are appropriately understood and that proportionate measures to mitigate them are incorporated into University strategies and plans

3. The Head of Data Protection and Information Compliance acts as the University's senior advisor and assessor on data protection issues. They hold the statutory role of Data Protection Officer and are the main point of liaison for external organisations and regulators relating to data protection. They monitor compliance with data protection within the University and ensure that the University is prepared to meet its DPA obligations. They also provide advice and guidance and formulate policies and procedures around effective information governance.

4. The Chief Information and Digital Officer (CIDO) oversees the effective management and security of IT resources, for example infrastructure and equipment. They formulate IT policies and procedures and ensure these are embedded within the organisation, developing and managing robust IT Security arrangements. They oversee the University's Business Continuity Plan.

5. The Associate Director IT Security and Business Continuity acts as the University's senior advisor and assessor on the security of data. They identify risks and manage corrective actions as well as managing security breaches and incidents.

6. The Head of Business Intelligence and Planning ensures that data needed for accurate gathering and reporting of business intelligence is fit for purpose, and that any use of data for analytics, reporting and business intelligence is in accordance with this policy.

7. Data Stewards have the responsibility to ensure the appropriate and effective management of data within their areas, ensuring it is fit for purpose and managed within the scope of legal and regulatory obligations and ultimately this policy. They lead and promote a culture that values and protects data across the University. Data Stewards will typically be at Director level. They may be supported by information managers within their areas who operate as Data Custodians.

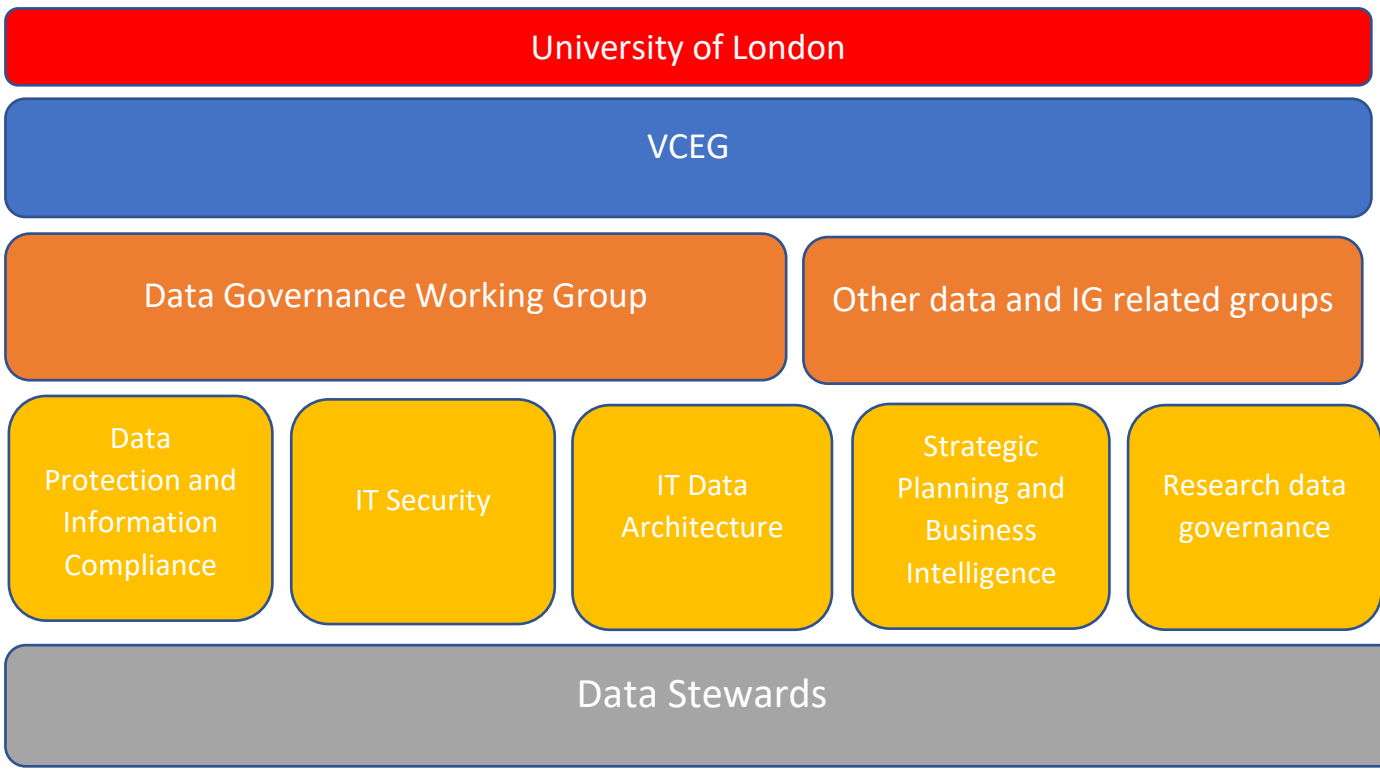
8. All managers are responsible for ensuring this policy is embedded within their departments and teams.

9. All users of data must ensure they follow the University's processes and procedures in handling data, including this policy and related policies.

10. Data governance shall be collaborative and transparent. Implementation of this policy will be overseen by an operational working group which includes representatives from ITDS, Data Protection and Business Intelligence. The working group will be overseen by the Director of Governance, Policy and Compliance. The Pro Vice-Chancellor (Partnerships and Governance) will attend as required and will report on implementation of this policy to VCEG. The working group will delegate as appropriate to other existing groups who operate in relation to information governance.

11. Additional descriptions of key roles can be found at Appendix 1.

12. The following structure forms an institutional Data Governance Framework:



5. Data Governance Guiding Principles and Objectives

This policy is underpinned by the following seven guiding principles and objectives :

Principle 1	**Data, in all forms, is recognised as a University asset**
Background	Data is managed as an important corporately owned asset with clear governance processes to control its processing. It is managed as a source of competitive advantage and is better protected and exploited.
Objectives	- There exists a benefit to or link through the use of data and the achievement of the University's goals and strategy. - The University culture is data driven with generally enhanced Data Management capability across the organisation with an increase in the number of data specialists in key areas. - Accurate management data is provided to enable effective University decision making. - The Data Governance Working Group provides oversight across the various groups responsible for data management - The IT Security Framework of policies is embedded. - Data Governance policies and guidance are embedded. - Enterprise data and other strategically important data held locally is managed for strategic, not local purposes. - Gaps in current resource and necessary University support to address them are identified.

Principle 2	**Data is held in compliance with the University's regulatory obligations including Data Protection**
Background	Data is kept secure and stored and handled appropriately to meet the requirements of legislation. Personal data must only be processed under appropriate, usually limited, conditions in compliance with Data Protection Legislation and other data driven statutory and regulatory requirements such as the OFS. Data subjects are able to exercise rights in respect of their own personal data.
Objectives	- The University is compliant with all current and emerging information compliance rules including the data protection legislation; - Categories of access to data are defined on a least privileged/need to know basis. - Data rights are able to be successfully fulfilled. - Data is managed in accordance with the University's IT Security Framework and Data Protection Policies - Effective vendor management and third party sharing due diligence ensures that all necessary agreements and assessments are completed and aligned to clear business need to legitimize data sharing.

	- Users are aware of, and adhere to, appropriate data security measures to assure the confidentiality, integrity and availability of University data - Users are aware of, and adhere to, governance policies and procedures around the appropriate storage and handling of data - Staff are empowered to seek guidance from specialist areas such as Data Protection &Information Governance and Cyber Security and know when and how to seek that guidance

Principle 3	**Confidence in the reliability and quality of the data is maintained throughout its lifecycle.**
Background	The University holds timely, accurate and reliable data in order to meet internal and external reporting requirements and to manage its activities and demonstrate accountability.
Objectives	- Personal data held by the University is accurate and inaccurate data is rectified or erased without delay. - Accurate external returns are submitted. - The funding requirements for the Office for Students and research grant requirements from private and public funders are met. - Extraction, manipulation and reporting of data is carried out to further University aims. Personal use of organizational data is prohibited.

Principle 4	**Data will be governed appropriately throughout its lifecycle in relation to its purpose**
Background	Data is assigned to a designated Data Stewards. It must be handled appropriately in line with University policies and procedures and kept appropriately secure. Personal data must only be collected for defined purposes and processed in compliance with Data Protection Legislation.
Objectives	- There is an understanding of data usage, flows against purposes and the data lifecycle is managed and documented. - Data is handled in accordance with University data security and data governance policies, procedures and guidance - A community of clearly defined Data Management roles are established and maintained. - The role and responsibilities of the Data Stewards are defined and the community of Data Stewards operates effectively across the University. - The community of appropriately trained and supported Data Stewards ensure that effective local protocols are in place to guide the appropriate use of data - Appropriate resourcing, training and organisational conditions are in place to ensure that Data Stewards can operate effectively. - Ethical aspects of data usage are considered as part of good data governance processes

Principle 5	**All data should be identifiable and managed**
Background	Data is identified, findable and managed in a structured manner and labelled and recorded in a consistent and logical fashion.
Objectives	- Data held within University systems and other networked locations is identified and personal data within that data is highlighted. - Interfaces, data flows, data modelling of systems and architecture support identification and management of data - Data is classified according to the data risk categories in accordance with the Data Classification policy. - Records retention schedules are established and all data will be managed in accordance with the agreed records retention policy - The management of data retention and governance is automated where appropriate. - Data is disposed of/archived appropriately.

Principle 6	**All data processing changes are subject to control**
Background	Measures are in place to ensure that changes to the processing of data are managed and go through appropriate change control and due diligence processes. These are referred to in relation any future changes to processing of that data.
Objectives	- The University's plans for the development of its technical architecture are driven by ITDS and Security policy frameworks and any changes will be properly controlled to reduce data compliance risk. - The criteria for managing and risk assessing changes to the way data is handled and processed is developed and embedded. - Changes to the processing of personal data will follow the Data Protection Impact Assessment process. - Changes to technical architecture are governed by the appropriate ITDS Change Advisory Board.

Principle 7	**The level of rigour is proportionate to the risk**
Background	The University's IT policy framework and other data governance polices within the University will inform data requirements. This Data Governance policy will ensure that the data collection, processing and sharing meets the needs of the University and effectively supports its mission while avoiding unnecessary bureaucracy or administrative burden. Controls and processes to manage data will be in accordance with these policies.
Objectives	- Data risk categories are clearly defined as reflected in the Data Classification Policy. - Data is appropriately classified, tagged, protected and managed according to its risk category. - Data management should be automated wherever possible.

	- Data Protection Impact Assessments clearly identify the risks to the University in all changes to processing of personal data and processes are in place to manage that risk appropriately. - Actions taken will be in proportion to the level of risk posed.

6. Relevant law, key policies and guidance

Internal

1. Glossary of Terms at Appendix 2.
2. Data Protection Policy
3. Records Management Policy
4. Information Security Policy
5. IT Acceptable Use Policy
6. HR Policies
7. Data Classification Policy and Guidelines

External

1. Data Protection Legislation (currently the UK GDPR and Data Protection Act 2018)
2. Privacy and Electronic Communications (EC Directive) Regulations 2003 and other relevant UK and EU ePrivacy legislation.

Appendix 1: Data Community Roles

Data Governance Working Group

1) Members of the Data Governance Working Group will be as follows:
   Chair: Director of Governance, Policy and Compliance
   Members: Head of Data Protection and Information Governance, Associate Director IT Security and Business Continuity, Director of IT and Digital Services, Head of Business Intelligence and Planning, Head of Management Information & Research Services (SAS), representatives from other relevant working groups, Pro Vice-Chancellor (Partnerships and Governance)

2) Main Purpose:
   a) To oversee, on behalf of VCEG, the development, implementation and review of information security, data management/ governance and data quality strategies and policies as well as organisational and technical measures to manage and protect the University's key corporate data assets with reference to relevant standards such as ISO15489, PCI-DSS, ISO27001, where appropriate.

   b) To review information risks to ensure that these are appropriately understood and that proportionate measures to mitigate them are incorporated into University strategies and plans

   c) To support the implementation of relevant policies and guidelines, including the data protection policy and the information security policy

   d) Support the implementation of an annual action plan.

3) Strategies and Polices and information compliance issues are escalated to VCEG (through PVC) as appropriate and for approval
   a) VCEG receive a report from the Working Group at least twice yearly
   b) Key decisions are escalated to VCEG as necessary

Data Protection Officer (DPO)

The role of DPO is statutory requirement currently undertaken by Head of Data Protection and Information Governance

1. Main purpose of the role:
   a) To act as the University's senior advisor and assessor on Data Protection and GDPR issues and the main point of liaison for external organisations and regulators for issues relating to Data Protection and information rights legislation. To monitor compliance with data protection requirements and ensure that the University is appropriately prepared to meet its DPA and UK GDPR obligations.

b) Lead the University's Data Protection and Information Compliance function.

c) To advise on information management and information governance matters and lead best practice in these areas.

2 Main duties:

a) To inform and advise the University and its employees about their obligations to comply with the data protection legislation and data protection requirements and to provide training.

b) To monitor compliance with data protection requirements and report any findings to the University Secretary

c) To act as first point of contact for regulatory authorities and other external organisations for all enquiries relating to data protection.

d) To act as the first point of contact for data subjects and to oversee any data subject access requests and complaints.

e) To inform and advise the University and its employees on information management and information governance best practice

Associate Director IT Security and Business Continuity

1. Main purpose of the role:

a) To act as the University's senior advisor and assessor on IT Security and Business Continuity issues and the main point of liaison for external organisations and regulators for issues relating to IT Security and Business Continuity.

b) Lead the University's IT Security and Business Continuity function

2 Main duties:

a) To inform and advise the University and its employees about their obligations to comply with the University's Information Security Policy and best practice behaviours.

b) To monitor compliance with the Information Security Policy and report any findings to the Director of ITDS and act as first point of contact for regulatory authorities and other external organisations for all enquiries relating to IT Security and Business Continuity.

c) To oversee the strategic and operational activities relating to IT Security and Business Continuity including Incident Management.

Chief Information and Digital Officer

1. Main purpose and duties of the role:
   a) Effective management and security of IT resources, for example, infrastructure and equipment
   b) The formulation and implementation of IT related policies and the creation of supporting procedures, ensuring these are embedded within the service
   c) The establishment of the Data Architecture models
   d) The establishments of the technical architectures that enable the creation, use and control of data.

Data Stewards

1. Main Purpose of the role:
   a. Leading and promoting a culture that values and protects data
   b. Understanding the data held and processed in their functional area and the purposes for which it is processed
   c. Understanding data flows relating to the data they are responsible for, while they are responsible for it
   d. Understanding and addressing the risks to the data while they are responsible for it
   e. Ensuring the data is used efficiently and effectively to achieve the vision of their department and the University
   f. Acting as the nominated "trustee" of an assigned data asset(s) on behalf of their department and the University
   g. Ensuring that the data is processed for purposes consistent with the strategic objectives of their department
   h. Determining how the data is collected, processed, retained and disposed of within their department in line with the overarching framework of the University; and
   i. Working with other Data Stewards to collaborate on internal data sharing arrangements.

2. Main duties:
   a. Review, at least annually (more frequently for higher risk information or assets with greater sensitivity), the data processing purposes for the data to ensure that it is kept up to date
   b. Ensure that all University data processing and information security policies and any University best practice guidance are followed
   c. Risk assess (if required) and log any changes to the processing of the data
   d. Report any known, suspected or potential data security or processing breaches to the Data Protection Officer, where appropriate
   e. Report regularly on information risk in your department and on any significant new processing changes or risks to the Data Protection Officer
   f. To attend available training

g. Keep a log of any new requests for access to the data

h. Work with other Data Stewards within the organisation to ensure that there remains a clear and documented framework of data asset ownership and a clear understanding of responsibilities and accountabilities – particularly in cases where data sets are transferred between Data Stewards

i. Provide an annual assurance to the University's Data Protection Officer that the data for which they are responsible is appropriately secure and has been used only for its stated purpose.

Data Custodians

1. Main Purpose of the role:
   a) Nominated by the Data Steward to support them in the execution of their responsibilities through their knowledge of data processing and data flows within their area

2. Main Duties:
   a) Provide information needed to review data processing purposes
   b) Provide information needed to create and update the framework of data asset ownership
   c) Support the annual assurance process

Appendix 3: Glossary of Terms and Definitions

Data: Data is a general term meaning facts and details that help to arrive at conclusions or which are processed to produce information

Data Architecture: The models, policies, rules, and standards that govern which data is collected and how it is stored, arranged, integrated, and put to use in data systems and in organisations.

Data or Information Assets: Sets of data held, created, maintained or otherwise processed for the University of London and maintained by Data Stewards as part of their responsibility to manage the data they hold.

Data Custodian Data Custodians support the Data Steward in the execution of their responsibilities. They have the primary administrative responsibilities for data assets within their functional area and have knowledge of data processing and data flows within that area.

Data Management: The development and execution of architectures, policies, practices and procedures in order to manage the information lifecycle needs of the University of London in an effective manner.

Data Protection Legislation: means (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the Data Protection Act 2018, the UK GDPR and all legislation enacted in the UK in respect of the protection of Personal Data as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (b) any code of practice or guidance published by the ICO (or equivalent regulatory body) from time to time;

Data Protection Officer: Named individual responsible for providing DPA advice and for acting as main liaison point with regulators.

Data Steward: Data Stewards have the primary management responsibilities for data assets within their functional area. Data Stewards are responsible for documenting the data they oversee, defining local procedures and making policy interpretations for their functional area(s).

Data Subject: an individual who can be identified, directly or indirectly by reference to an identifier; an individual about whom data relates.

Personal Data: Data which relates to a living individual who can be identified from the data, or from that data in combination with other data held by an organisation

Processing: any operation or set of operations which is performed on data or on sets of personal data such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction.

Special Category Data: Data as described in the UK GDPR which relates to a living individual of a sensitive nature, particularly concerning their racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offence.