Data Governance Procedure

Related College Policies	Data Governance Policy Data Protection Policy Records Management Policy IT Acceptable Use Policy Research Data Management Policy
Related Procedures	Data Protection Procedure Data Breach Management Procedure IT Acceptable Use Policy - Email Procedures Information Classification Procedures

---

1.0 Implementing the Data Governance Policy

1.1 Data Stewards and Data Custodians are responsible for setting processes for how data they manage are used.

1.2 Data users need to escalate any substantial data issues with datasets that result in poor quality data or require excessive data cleansing before the data is usable. Any business impacting data issues will be reported to Data Stewards and appropriate Data Custodians who will oversee stakeholder engagement and resolution.

1.3 The Data Governance Committee will determine what data will undergo a data audit.

2.0 Scope

2.1 This procedure applies to all institutional data used in the administration of the university and all of its organisational units for College business except data used for the purpose of academic research, where the principal investigator is responsible for governance of their data.

2.2 This procedure covers, but is not limited to, institutional data in any form, including print, electronic, audio-visual, backup and archived data.

2.3 All staff using institutional data must adhere to Data Governance Policy and Procedures.

3.0 Purpose and Goals

3.1 Data Governance will help the College achieve:

- accurate reporting and understanding of the data held;
- efficiency due to a reduction of human intervention required to check data;

- reduced costs as staff time won't be spent checking data;
- improved relationships with suppliers;
- accurate data;
- standardized data systems, data policies, data procedures, and data standards;
- natural compliance with the law through BAU processes;
- increased transparency within any data-related activities;
- processes where if data inaccuracies are noticed, they can be fixed at the central source where the data is held and not just fixed locally in local reports;
- identification, documenting and resolution of past and current data issues.

4.0 Data Governance Principles

4.1 Staff responsible for making decisions based on data available will adhere to the data governance principles. The principles are as follows:

- Data is a valued university asset
  Data must enhance the experience of staff and students. It must be trusted, documented how to manage, ethically managed and have clearly defined purposes in support of the university's strategic aims.
  Data collected and used by the university is a critical resource, central to our success. It is considered and valued in the same way as other valued assets such as people, Intellectual Property rights, buildings or money.

- Data Transparency
  The College will lead by example to be transparent in its decision-making and publication where possible. This includes proactively publishing information and publishing data requested under the FOI Act. Any information or communication relating to the processing of data is accessible and easy to understand with clear language used.

- Data Quality
  Data will need the right quality for its intended use. It is not required to be perfect, only that its quality characteristics are pragmatic, appropriate, and transparent. Data can be accessed and analysed simply and quickly. Data Duplication should be kept to a minimum. Where possible data should not be stored outside of its designated location for example on personal drives, OneDrive. Retention, classification and access control procedures apply to data regardless of its location.

- Data Accessibility
  The default accessibility of data is open, so it can be made available to the maximum number of people for the greatest number of uses. However, this availability must be considered in terms of proportionality and need. It is easy to find data you need when and where it is needed for business purposes. Finding information on data stewards/policy/definitions is straightforward and intuitive.

  Data Accessibility does not contravene the university's responsibilities under the Data Protection Policy. The College will always protect data and ensure appropriate

security and access controls as appropriate in line with the Data Protection Policy and Information Classification Procedures. Where data is extracted from a system or is held outside the normal location, the data shared needs to be managed in line with the access controls, classification, and retention policy from where it was originally sourced.

- Contextual Data Management
  Data will be efficiently managed at all stages; from identification of need, creation or collection, storage, sharing, protection, and use taking account of value and risk.
  Our culture will support discipline and professionalism across the data supply. Data will be managed according to its value and cost. Data integrity will be maintained ensuring one true copy of data is maintained with a single version of the truth.
  Data is governed and accountability is understood, respected and embedded in all our processes.

- Data Definitions
  Data will use standard methods of recording individual data items across the University purposes and across systems with clear ownership and process to ensure maximum reuse and sustainability.
  Data will be standardised, so it can be compared to data drawn from other systems and linked to create usable and informative datasets. A common language to underpin productive discussions about data will be developed through well-defined purposes and shared definitions.

5.0 Data Quality Test

5.1 Questions to assess the quality of data are:

- If it has sufficient granularity to allow trends to be identified and a full reading of the dataset;
- it is free from mistakes, errors and omissions;
- the recording of data are adequate, performed in a timely manner and is kept consistent across time;
- it is consistent with other relevant internal and external data;
- data are to a large degree consistent in time with a different output based on several data sources refers to a well-defined point in time;
- a high level of confidence is placed on the data making it usable for operations and decision-making processes;
- sufficient historical data are available;
- no relevant data available is excluded from consideration without justification;
- it fulfils all of the requirements for those who use the data;
- a comparison with other data of other institutions to establish are there ways of improving the dataset.

5.2 Where data is essential to the university, data quality issues can be reported through the service desk or to the appropriate Data Steward.

6.0 Data Governance Maturity

6.1 Not all data is equal and as outlined in the table below, different types of data will have different impacts on the organisation and different levels of proactive management of that data will be expected.

6.2 Data should be known and mapped out to determine where and how it is used.

6.3 For departments who hold or gather a large amount of university data, a data models should be in place showing how data is collected and what is done with the data through the data model. In some instances, there will be overlap between departments as one dataset may be used for numerous tasks.

6.4 The below table includes 3 categories of data types and data management will be based on the importance of the data to the organisation. Data Stewards have ultimate responsibility for assigning a level of importance and maturity to data types.

Data Structure	Meaning	Governance Expectation
Structured Data	The data has a material effect on executive decision making, capital modelling, technical provisions, and regulatory reporting.	Data is known and understood by the university on where it is stored and how it is used. The data has appropriate access and retention controls. Managed fully in accordance with Data Governance Policy with named Data Stewards and Data Custodians. This should have a Proactive State of Maturity.
Semi-Structured Data	Data that may be held in systems used for limited purposes and the data are not material to executive decision making but may be material to other business uses. The full data management cycle of the data may not be known but it does not have any negative impact on its value or how it is used across the university.	Data Governance will be enacted after an issue is raised in a particular area, but proactive data governance will not take place. This should have a stable-proactive level of maturity depending on the purposes the data is held for and its importance to the College.
Unstructured Data	Data such as draft documents that does not have a material effect on business operations, for example, for example data held in personal drives. The data is	Fixes may be requested, but no ongoing monitoring will take place. This should have a reactive – stable level of maturity depending on the

	generally used for short term tasks. Once the data is no longer required, it is deleted.	purposes the data is held for and its importance to the College.

6.5 The Data Governance Maturity Assessment helps Data Stewards and Data Custodians how mature their data governance regime is and help them determine where they want to get to for their data.

6.6 Essential data for conducting day-to-day College should managed in a proactive state.

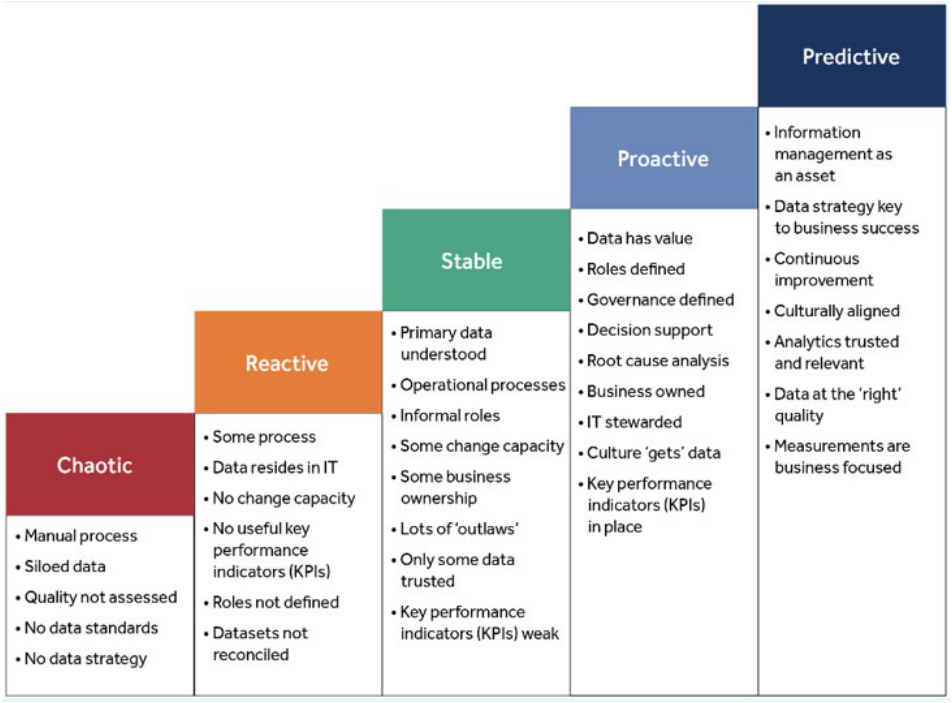

Figure 1 - Data Governance Maturity Scale

7.0 Core Data Domains

7.1 The core data domains identified in the below table represent a high-level overview of the main categories of data held by the College and lines of responsibility. This list is not exhaustive.

Data Domain	Data Steward
Alumni & Fundraising	Executive Director, Fundraising & Supporter Development
Digital Environment	Chief Information Officer
Education and Students	Executive Director, Education and Students
External & Internal Engagement	Director of Brand & Marketing
Finance and Commercial	Chief Financial Officer

Health & Safety	Director, Health & Safety Services
Libraries & Collections	Executive Director, Education and Students
People and Organisation	Director of Human Resources
Physical Environment	Director of Estates & Facilities
Relationships and Communication	Director of Brand & Marketing
Research & Researchers	Operations Director (Research & Researchers)
Strategy, Planning and Analytics	Director (Strategy, Planning and Analytics

8.0 Review Process

8.1 The Data Governance Committee will do annual assessments of overall data governance maturity and note improvements. The Data Governance Committee has responsibility for ensuring the Data Governance Policy & Procedure is implemented and reviewed at least bi-annually.

Appendix 1 - Roles and Responsibilities

1.0 Data Steward

1.1 Data Stewards are members of staff who are appointed responsibility and accountability for the management of specific datasets which are relevant to their directorate/faculty. Data Stewards vocalise issues with datasets. The dataset may be used by other departments in King's. Data Stewards understand the data used operationally and the purpose it serves.

1.2 The Data Steward will:

- Provide strategic direction and oversight over how to maintain and improve the data available and the way it is used by the organisation.
- Use College procedures for requesting, approving, and revoking data access.
- Coordinate their work with other stakeholders for example with IT, for the security of data.
- Be informed and aware of downstream data uses or analytics, with data flows and oversight reported to Data Stewards or nominated Data Custodians.
- Receive regular updates and support from Data Custodians about operational data governance of their datasets.
- To oversee the overall management, integrity of university data, ensuring it is accurate, up-to-date, and trusted by all members of the university community and external stakeholders.
- Form a network of stakeholders for a dataset to ensure the policies and procedures of data governance for that dataset are upheld and fit for purpose.

2.0 Data Custodian

2.1 The Data Custodian receives delegated authority from the Data Steward for the operational management of their datasets. A Data Steward may have numerous Data Custodians reporting to them, for example the Workforce Data Steward may have a different Data Custodians for recruitment and for payroll.

2.2 Data Custodians will have day-to-day responsibility for:

- Data security - knowing where data is held and that it is safe. Any breaches of unlawful disclosure/access to the data are to be reported immediately to the data steward and information compliance team.
- Access – knowing the profiles of access to the data, why they use it, and who do they pass the data to.
- Coordinate with other users of the data to know any issues that may exist or arise with the dataset. For example, if a piece of data from the dataset was removed because the central team did not need it, data custodians need to consider if this would this have knock on effects for data users outside of the core team who also use the data.

- Integration of data gathered through different channels. Data Custodians should be aware of similar data gathered by other departments and ensuring the datasets can be integrated if needed, for example if a faculty learned that a student was deferring a year of their course, the data held by the central team needs to reflect this.
- Data custodians will prove accountability through documentation such as data mapping or data protection impact assessments as it will detail how the data is sourced and used by the organisation.
- Creating and capturing accurate data, based on the needs of Data Users or recording known issues with data and the consequences.

3.0 Data Governance Committee

3.1 The Data Governance Committee will provide a central group with oversight of what data is held by the organisation and provide a path to improve and maintain the quality of the data held. The Committee will be predominately made up of Data Stewards.

4.0 Data Governance Manager

4.1 This role will be part of the Information Compliance team who will be responsible for the Data Governance Framework, up to date membership, and driving forward issues prioritised by the Data Governance Committee.

5.0 Data Users

5.1 These are individuals in the university who use datasets as part of university business. They are not responsible for collecting, storing or ensuring the reliability of the data. Data users are usually the most familiar with the data quality issues of datasets they use. Data Custodians should regularly communicate with Data Users to understand the issues with datasets to understand how to fix them.

6.0 Data Facilitators

6.1 Data Facilitators help Data Stewards and Data Custodians meet their responsibilities under data governance. Data Facilitators are not responsible for the dataset and usually they don't use it. IT would usually be a Data Facilitator as they are not usually solely responsible for the data collected, but they assist in planning the data to be gathered and how best to appropriately store data. IT would usually assist in ensuring the data collected and stored is fit for purpose and that it is kept secure. Data Facilitators aim to understand the requirements set out by Data Stewards and Data Custodians to improve a dataset and Data Facilitators architect a way forward and, in some instances, implement the plan.

Appendix 2 - Glossary of terms:

Cyber Security	Cyber Security is the combination of people, policies, processes, and technology employed by an enterprise to protect its cyber assets.
Data	Any symbols or characters that represent raw facts or figures such as numbers, words, measurements, observations, or description of things [2].
Data Access	The ability to interact with data in one or more ways, such as the ability to read, copy, query, retrieve, update or delete data.
Dataset	Logically meaningful grouping of data[3]
Data Dictionary	A collection of entries where an unambiguous identifier with a term and definition are laid out[4]
Data Governance	Proactively managing the quality, consistency, usability, and availability of data and subsequent information through an accountability framework[5].
Data Protection Act 2018	UK law which sets out the framework for data protection. It sits alongside and supplements the UK GDPR[6].
Data Quality	A set of inherent characteristics of data fulfills pre-determined requirements[7]
Data Quality Management	Co-ordinated activities to direct and control data quality across an organisation[8]
Information Security	Preservation of confidentiality, integrity and availability of information systems; as well as other properties such as authenticity, accountability, non-repudiation[11].
Information Security Policy	Document that states, in writing, how an organisation plans to protect its physical and information technology assets[12].
Metadata	Defining and describing other data[13]
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[14].
Data Users	Anyone accessing university-owned information, including data held electronically and paper-based records. This could include, but is not limited to, staff, students, governors, contractors, partners, and collaborators.
UK General Data Protection Regulation (GDPR)	UK law which came into effect on 1 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK. It is based on the

EU GDPR which applied in the UK before that date, with some changes to make it work more effectively in a UK context[15].