Institutional Data Governance Policy

Scope
This document sets out the policy and framework to be followed to manage Institutional Data and applies to data in all its forms.

Status and Effective date
Approved, April 2015
Validity: under annual review.

Audience
This policy applies to everyone at the university and sets out responsibilities for Stewards, Custodians, and Users of Institutional Data.

This policy informs governance forums and decision makers for key university resources; such as people, process, technology, data and space. Those involved in university processes, Business Continuity, Information Compliance, Reporting, Decision Support and a range of other functions and stakeholders all benefit from well-governed data. The IT architecture and strategy is informed by and supports the goals of Data Governance.

Purpose and Goals
Institutional data is key to data-driven decision making, identifying new opportunities, planning and g risk management. Processes and Technology depend on Institutional Data. They transmit, use, transform and supply Data to support University strategy and operations.

Institutional Data is a strategic asset of the University and shall be managed according to sound data governance procedures and approved principles. A set of applicable principles relating to data and broader aspects of governance is maintained by ITGS in conjunction with DGSG.

In accordance with this policy DGSG shall assign stewardship responsibilities for university data; establish standards for the custodianship of such data.

Benefits of applying this policy will include ensuring data is fit for the purposes of internal and external reporting, and is appropriately categorised for storage, retrieval, destruction, backup, and access as needed to ensure proper management and protection of Institutional Data; with the goals of:

- Enabling better decision-making;
- Reducing operational friction;
- Protecting the needs of data stakeholders;

Summary
Everyone has a responsibility to look after university data, and abide by DGSG policy, and all applicable laws including the Data Protection Act. Data matters because it is the lifeblood of business processes and is used to make decision. Everyone uses data in what they do (processes) and often this data is provided by (IT systems) technology. Mismanagement of data by students, staff or others may lead to fines, reputational damage, and can have other process and financial implications.

DGSG looks after Data Governance and Strategy and is accountable to PET.

DGSG appoints senior level individuals as Data Stewards look after particular sets of data, such as “people data”, “student data”, and so on. For example the HR Director is a suitable Steward for People Data.

Data Stewards shall appoint Data Custodians as required to assist in the execution of the data strategy, policy and procedures for their area of stewardship.

A number of groups work together, and report to DGSG, to look after particular areas of data, such as statutory management returns, research management data, and user groups for decision support.

DGSG provides IT with requirements to support Data Governance including Decision Support. IT deliver those requirements through the IT Roadmap and associated technical decisions and standards governed by ITGS.

Since data is central to what we do, and we all use or create data, a number of principles help us all in our decisions and use of data.
Institutional Data Governance Policy

- Training management and staff to adopt common approaches to data issues;
- Building standard, repeatable processes;
- Reducing costs and increasing effectiveness through coordination of efforts;
- Ensuring efficiency and transparency of processes;
- Informing business continuity (ensuring the ongoing availability and disaster recovery of key data);
- Supporting IT roadmap planning and technical decisions;
- Reducing the risk of mismanagement of data by students, staff or others; which may lead to fines, reputational damage, and can have other process and financial implications.

Governance Roles and Responsibilities

No one person, department, division, school, or group “owns” Institutional Data, even though specific units bear some responsibility for certain data. The University owns the data (or in some cases, such as with National Security numbers, is the custodian of data), but a specific person in the form of the Steward has ultimate responsibility to define management of the assigned data set within the scope of legal and regulatory obligations. The roles and responsibilities outlined below will govern management, access, and accountability for Institutional Data and will be assigned by the DGSG.

Institutional Data Governance

DGSG looks after Data Governance and Strategy and is accountable to PET.

The University Secretary appoints Committee members, who include representatives from Academia, Research and Information Technology and senior University management. The DGSG may create further subcommittees and task forces as needed.

Data Governance shall be collaborative and transparent.

Relationship between Governance Bodies and Governed University Resources

None of the university’s key resources (people, process, data, technology and space) can be considered in isolation: Effective investments in the university are often multi-faceted. Changes to people, process, space, technology and data must be actively governed and co-ordinated across academic and support disciplines. The university has adopted the COBIT and TOGAF frameworks for governance and architecture. Best practice principles from these frameworks have been adapted and adopted by ITGS and apply across the governance and planning of business process, technology and data.

DGSG shall direct, monitor and evaluate Data, ensuring appropriate reference and collaboration with the other key resources governed outside of DGSG immediate remit: particularly people, process, technology, space, and the relevant governance vehicles as applicable. This supports holistic and end to end outcomes for the University.

1. PET / EPET set overall direction
2. ITGS governs (evaluates, directs and monitors) IT and IT Data Architecture. ITGS ensures university wide review for the King’s approach to managing process and the associated activity model. This provides an organisationally neutral holistic model. ITGS provides a single governance framework through for university-wide IT Architecture, Roadmap, Procurement and Standards
3. Information Security Group addresses university wide information security policies, performance and issues
4. DGSG directs all matters for KCL data governance. Includes Data Stewards, IT and Management/ Returns Reporting. DGSG governs Data Strategy in partnership with IT (for Data Architecture and Systems Implementation).
5. Data Governance Focus Groups form on an ad hoc or project basis around domain areas, such as HR, Finance, Student data. Some groups may be standing groups such as Management Information & Reporting. This also includes any relevant user groups such as Decision Support (Insight User Group).

6. Statutory Returns Management Group oversees processes and procedures associated with statutory returns

7. SRM sub-groups as required oversee individual returns

8. King’s Futures, Faculty and Directorate Strategies provide requirements that DGSG and ITGS take into their work: shaping and impacting policies, procedures and roadmaps.

9. Business Continuity Planning Group (chaired by Estates) to ensure that management of data is adequately factored into emergency preparations

D – Close alignment between ITGS and DGSG ensures IT Architecture supports the Data Vision and joint agreement on Data Policies and Strategy. DGSG ensures that Data Management leverages the ITGS approved Decision Support Strategy, capabilities and roadmap for IT Data Support.

King’s Governance Principles for Data

Principles apply to all forms of data governance and planning, and guide governance decisions, process and systems development. DGSG shall ensure that an approved set of principles for data is reviewed, agreed and is compatible with other data requirements. The principles relating to data and broader aspects of governance is maintained by ITGS in conjunction with DGSG. Data policies that impact general Information Security shall be reviewed and approved by the Information Security Forum.

Principles help stakeholders make data-related strategic and tactical decisions within and across Data Domains. The current set of ITGS approved principles is maintained on sharepoint here and is summarised below.

- Data is an Asset - Data is an asset that has value to the University and is managed accordingly. Look after data and protect it.
- Data that has shared value should be shared - Users have access to the data necessary to perform their duties; therefore, data is shared across University functions and organizations. Use of data shall comply with the direction set by the Data Steward (e.g. people data shall be handled in accordance with the direction set by the people data steward, wherever that data is held in the university)
- Data is Accessible - Data is accessible for users to perform their agreed functions when and how they need it.
- Data Trustee - Each core University data element has a trustee accountable for data quality.
- Common Vocabulary and Data Definitions - Data is defined consistently throughout the University, and the definitions are understandable and available to all users.
- Data Security - Data, whether stored, in transit or in use, is protected from unauthorized use and disclosure to ensure the required levels of confidentiality, integrity and accessibility
- Interoperability - Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology.

Law, regulations and standards

Nothing in this policy precludes the disclosure of Institutional Data to external organizations, governmental agencies, or authorized individuals as required or permitted by legislation. The university’s policies on disclosure and personal data should be consulted as appropriate, available through the Policy Zone
Institutional Data Governance Policy

Data shall be managed with due regard to all applicable laws and regulations, as well as relevant best practice frameworks. Of particular note is the Data Protection Act, which controls how your personal information is used by organisations, businesses or the government.

Everyone responsible for using data has to follow strict rules called ‘data protection principles’. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- maintained in an accurate state
- kept for no longer than is absolutely necessary
- handled according to people’s data protection rights
- kept safe and secure
- not transferred outside the UK without adequate protection

There is stronger legal protection for more sensitive information, such as:

- ethnic background
- political opinions
- religious beliefs
- health
- sexual health
- criminal records

Reference shall be made to relevant standards, such as ISO27001, the best practice standard for Information Security, with the specific aims of ensuring data is appropriately managed and safeguarded to ensure appropriate Data Confidentiality, Integrity, and Accessibility.

Reference shall also be made to Higher Education bodies such as HESA, HEFCE or JISC where collaboration or other models may prove useful to the University.

The Director of Governance and Legal Affairs Management has responsibility for interpreting the laws governing data access and related issues.

Personal responsibility

All users of data have responsibility for preserving the security and integrity of Institutional Data. Proper stewardship and custodianship of university Institutional Data will facilitate appropriate access to data. All data users must adhere to the following:

- **Confidentiality**: Respecting the confidentiality and privacy rights of individuals whose records they may access.
- **Ethics**: Observing the ethical restrictions that apply to data to which they have access.
- **Policy Adherence**: Abiding by applicable laws and University policies with respect to access, use, protection, proper disposal, and disclosure of data.
- **Quality Control**: Reviewing reports created from data to ensure that the analysis results are accurate and the data has been interpreted correctly.
- **Responsible Access**: Accessing and using Institutional Data only as required in their conduct of University business. Reporting any breaches of University information in a timely manner according to procedures defined in the Incident Management Policy.

Change Management

Modifications to the approach, reference data values and the structure/use of master data, metadata and models used for Data Governance will be change-managed through DGSG.
Data Strategy

A vision statement and plan for data strategy shall be maintained. This sets priority and direction for data and data-related activities. Such strategy will take into account the overall university approach for the deployment and development of its key resources: people, process, technology, data and space.

Technology for Data

DGSG shall specify and prioritise the requirements and strategy for data management. The technology to implement those requirements and strategy shall be specified and implemented by IT as part of the IT Roadmap for Projects and Improvements. DGSG shall prioritise the Decision Support section of the roadmap as part of the overall IT prioritisation via ITGS. DGSG shall review and validate a record of University Data and Solution owners and stakeholders for each application on the IT Portfolio. IT shall create and maintain this record.

User groups for Data Technology and Decision Support

DGSG shall sponsor and direct user groups as required for Data Technology and Decision Support. They shall comprise representatives from across the University and include “user” and IT representatives. They shall make recommendations to DGSG to support the development of Data and IT Strategy. They shall assist the University in the realisation of the approved and agreed Strategies and making best use of the available capabilities (people, process, technology etc.)

Data Stewards, Custodians and Statutory Returns Managers

DGSG shall appoint Data Stewards and ensure that all relevant Data Entities have a responsible Steward, and ensure Statutory Returns Managers are appointed. A Data Steward or Custodian may be assigned the role of a Statutory Returns Manager.

Data Stewards look after particular sets of data, such as “people data”, “student data”, and so on. Data Stewards shall be responsible for the management of data under their oversight, under the direction of the DGSG. They shall appoint Data Custodians as required to assist in the execution of the data strategy, policy and procedures for their area of stewardship.

Use of data from one domain by another (sometimes known as transformed data) shall comply with the direction of the steward for the data as per the source. For example, the rules, definitions and treatment of people data, wherever that data may be held shall comply with the rules, definitions and treatment established by the people data domain owner.

The responsibilities of Data Stewards, Custodians and Statutory Returns Managers are elaborated in appendix: terms and definitions.

Data Classification

DGSG shall ensure that there is an approved Data Classification classifying each data element according to an agreed university definition; an example of this definition might be Sensitive (high risk), Restricted (medium risk) and Public (low risk).

Institutional Data Model

DGSG shall oversee the university Institutional Data Model, including the definition of different types of institutional data, and defining the standard for documentation of data elements. This includes documenting data flows between systems and organisations so the origin of data elements can be traced through organisational systems and processes.

The types of institutional data will align with the King’s Activity Model wherever possible. The key value-adding activities areas are in the academic endeavour: Education and Research. The supporting activities are Support and Administration, Collaboration and Infrastructure. Partners may be a value-add activity or support, depending on the nature of the partnership.
Access to Data

Institutional Data is available to individuals carrying out their University responsibilities on an as needed basis. An individual interested in utilizing Institutional Data for any other purpose must request the Institutional Data through a Freedom of Information request.

Appendix: Terms and definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role:</td>
<td>DGSIG shall appoint Data Stewards and ensure that all relevant Data Entities have a responsible Steward.</td>
</tr>
</tbody>
</table>
| Data Stewards      | Data Stewards look after particular sets of data, such as “people data”, “student data”, and so on. For example the HR Director is a suitable Steward for People Data. Data Stewards shall be responsible for the management of data under their oversight, under the direction of the DGSG. They shall appoint Data Custodians as required to assist in the execution of the data strategy, policy and procedures for their area of stewardship. Use of data from one domain by another (sometimes known as transformed data) shall comply with the direction of the steward for the data as per the source. For example, the rules, definitions and treatment of people data, wherever that data may be held shall comply with the rules, definitions and treatment established by the people data domain owner. Stewardship can be considered as:  
  • Taking responsibility for the survival and wellbeing of something that is valued.  
  • The responsibility for taking good care of resources entrusted to one.  
  • The science, art and skill of responsible and accountable management of resources.  
  • Being responsible for managing property or resources; the individual's responsibility to manage his/her life and property with proper regard for the rights of others.  
  • The practice of managing or looking after the wellbeing of something.  

Stewards of Institutional Data have the primary administrative and management responsibilities for segments of Institutional Data within their functional areas. Stewards of Institutional Data implement policy, define procedures pertaining to the use and release of the data for which they are responsible, and ensure the feasibility of acting on those procedures. Stewards are responsible for defining procedures and making policy interpretations for their business unit(s). Any such business unit specific items must, at minimum, meet University policy standards. They are responsible for coordinating their work with other university offices associated with the management and security of data, such as the Information Security Officer and IT staff. Access: Approving requests for access to Institutional Data within their functional area, specifying the appropriate access procedure, and ensuring appropriate access rights and permissions according to classification of data. Communication: Ensuring that Consumer/Users of the data for which the Stewards are responsible are aware of information handling procedures. Compliance and Data Security: The Steward is ultimately responsible for compliance with applicable legal and regulatory requirements, and with University policies and procedures, including specific policies or procedures established by Information Security, ITGS and DGSG. Stewards must be knowledgeable about applicable laws and regulations to the extent necessary.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>to carry out the stewardship role. Stewards must take appropriate action if incidents violating any of the above policies or requirements occur</td>
<td></td>
</tr>
<tr>
<td>• Data Classification: Classifying each data element according to University definition - Sensitive (high risk), Restricted (medium risk) and Public (low risk).</td>
<td></td>
</tr>
<tr>
<td>• Data Lifecycle and Retention: Ensuring appropriate generation, use, retention, disposal, etc., of data and information consistent with University Policies, among them the Information Security Policy and standards for disposal.</td>
<td></td>
</tr>
<tr>
<td>• Data Manipulation, Extracting and Reporting: Ensuring proper use of Institutional Data and recommending appropriate policies regarding the manipulation or reporting of Institutional Data elements (in line with reporting standards established by the ITGS and DGSG) and implementing business unit procedures to carry out these policies.</td>
<td></td>
</tr>
<tr>
<td>• Data Quality, Integrity and Correction: Ensuring the accuracy and quality of data (access control, backup, etc.) and implementing programs for data quality improvement. Developing procedures for standardizing code values and coordinating maintenance of look-up tables used for Institutional Data. Consulting with data consumers / users to determine appropriate data sources. Determining update precedence when multiple sources for data exist. Determining the most reliable source for data.</td>
<td></td>
</tr>
<tr>
<td>• Data Storage: Documenting official storage locations and determining archiving and retention requirements for data elements.</td>
<td></td>
</tr>
<tr>
<td>• Education (Training and Advice): Ensuring that education of employees responsible for managing the data is provided in reporting standards, data retention, data handling, and data security.</td>
<td></td>
</tr>
<tr>
<td>• Policy Implementation: Establishing specific goals, objectives, and procedures to implement the policy and monitor progress toward implementation.</td>
<td></td>
</tr>
<tr>
<td>Role: Data Custodians</td>
<td>Data Custodians are university officials and their staff who have operational level responsibility for the capture, maintenance, dissemination and storage of Institutional Data. Stewards of Institutional Data may appoint Custodians to assist with data administration activities. A Custodian of Institutional Data is given specified responsibilities and receives guidance for appropriate and secure data handling from the Stewards. A Custodian has the responsibility for the day to day maintenance and protection of data. Specific responsibilities also include:</td>
</tr>
<tr>
<td>• Access: With guidance from the respective Stewards and in collaboration with technical support staff and University Counsel, Custodians recommend appropriate procedures that satisfy specified information security requirements including legal and compliance obligations as well as applicable University policies.</td>
<td></td>
</tr>
<tr>
<td>• Coordination: With guidance from the respective Stewards and in collaboration with technical support staff and University Counsel, Custodians recommend appropriate procedures that satisfy specified information security requirements including legal and compliance obligations as well as applicable University policies.</td>
<td></td>
</tr>
<tr>
<td>• Data Collection and Maintenance: Collecting and maintaining complete, accurate, valid, and timely data for which they are responsible</td>
<td></td>
</tr>
<tr>
<td>• Data Security: Administering and monitoring access in collaboration with technical support staff, defining mitigation and recovery procedures. Reporting any breaches of University information in a timely manner in accordance with the Incident Management Policy. Coordinating data protection with the Information Security Office as necessary.</td>
<td></td>
</tr>
<tr>
<td>• Documentation: Writing the documentation for each data element based upon stewardship requirements, policy, and best practices. This documentation will include, at a minimum, the data source, data provenance, data element business name, and data element definition. It should</td>
<td></td>
</tr>
</tbody>
</table>
### Term | Definition
--- | ---
| | also include documentation of reporting processes, and the basis for data categorisations within these processes (for example, categorisation of student and staff activity, or of expenditure data).
| | • Education (Training and Advice): At the direction of the Steward, providing education in data retention, data handling, and data security to employees responsible for managing the data.

**Role**

| Statutory Returns Managers | The Return Mangers for the statutory returns should ensure the following:
| | • Processes exist for gathering new/changed data requirements in a timely manner and ensuring deadlines are met.
| | • HESA’s check documentation is reviewed in detail by someone other than the principal return compiler, and any highlighted issues (e.g. significant year on year changes) are addressed through further data and sense checking as necessary.
| | • Data in the returns are optimised and aligned with other statutory returns to ensure institutional consistency.
| | • All errors and warnings identified by HESA via the ‘Minerva’ database are addressed in a timely manner and with appropriate detail (e.g. provide explanations of why apparently anomalous data is correct)
| | • Initial data quality improvement priority lists are produced prior to first submission of the return, for review by SMRG and by Line Managers or Accountable officers.
| | • Data quality summaries are produced following the ‘Commit’ stage, for review by the SMRG.
| | These should include:
| | - Success in addressing data quality issues, level and materiality of risk attached to issues that will take longer to address, and plans for further data quality improvements in the short term and in subsequent years.
| | - Deadlines met/not met to date.
| | - Summary progress on Minerva queries & plan for resolving outstanding queries.
| | - Confirmation of plans for formal sign off through Accountable officers.

Where there are concerns that the resources are not in place to execute the responsibilities above, the Return Mangers for the statutory returns will raise this with line managers in the first instance.

Where there are concerns that outstanding data quality issues present material risks to the integrity of the return, the Return Mangers should raise this with their line manager in the first instance, who in turn should raise this with the Accountable officer. This should be done in a timely manner (at least 4 weeks before the last submission date).

Accountable officers should:

- Confirm to the Principal, through the DG&SG, that a data quality assurance process has been followed and returns can be signed off by the Head of the Institution.
- Review proposals for system changes to improve data quality and prepare appropriate responses.
- Ensure there are effective mechanisms for statutory requirements to be incorporated into system development programmes/projects.

**Access**

Access is the right to read, enter, copy, query, download, or update data.

University employees or agents must be granted access to data elements according to the procedures specified by the Steward of that data and consistent with applicable laws and regulations.

Users desiring data shall submit a completed form requesting access and acknowledging responsibility to the Steward of that data. The form contains the appropriate level of approval as determined by the Steward. If approval is granted, the Custodian will enter the User’s credentials into a registration system, allowing access. If warranted, the Steward or Custodian will seek additional approvals. The DGSG will set policy for access to Institutional Data.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedures</td>
<td>Procedures shall be defined and documented by Stewards to permit access to data elements in Institutional Datasets, and authorised by DGSG</td>
</tr>
</tbody>
</table>
| COBIT                       | COBIT is the leading best practice framework for governance that where information is a key resource for enterprises. From the time that information is created to the moment that it is destroyed, technology plays a significant role. Information technology is increasingly advanced and has become pervasive in enterprises and in social, public and business environments. COBIT practices help organisations govern the related aspects of process, information and technology.  

COBIT helps enterprises and their executives to:  
- Maintain high-quality information to support business decisions.  
- Generate business value from IT-enabled investments, i.e., achieve strategic goals and realise business benefits through effective and innovative use of IT.  
- Achieve operational excellence through the reliable and efficient application of technology.  
- Maintain risk at an acceptable level.  
- Optimise the cost of services and technology.  
- Comply with ever-increasing relevant laws, regulations, contractual agreements and policies. |
| Compliance                  | The Steward is ultimately responsible for compliance with applicable legal and regulatory requirements, and with University policies and procedures, including specific policies or procedures established by ITGS and DGSG. Stewards must be knowledgeable about applicable laws and regulations to the extent necessary to carry out the stewardship role. Stewards must take appropriate action if incidents violating the above occurs. |
| Conflict Resolution         | DGSG will govern and arbitrate the definition of centrally-used administrative data attributes, data policy, and categorisation of data for internal or external reporting purposes, and levels of access are resolved, particularly for data elements that cross stewardship boundaries. In resolving these conflicts, DGSG would commission and draw on relevant analysis of business systems and processes and assess the impact (or potential impact) of particular policies or procedures on the University’s performance. |
| Data                        | Data in all its forms is subject to DGSG governance (including but not limited to machine readable data, data in electronic communication systems, data in print, and backup and archived data on all media).                                                                                                                                                                                                                                                      |
| Data (information) Security | Data Security includes administering and monitoring access in collaboration with technical support staff, defining mitigation and recovery procedures. Reporting any breaches of University information in a timely manner in accordance with the Incident Management Policy. Coordinating data protection with the Information Security Office as necessary.                                                                                                                                                                                                                                     |
| Data Administration         | Ensuring formal guidelines and tools are used to manage the University’s data resources. Ensuring all Institutional Data has an identified Steward who effectively oversees the administration and management of all Institutional Data for which they are responsible.                                                                                                                                                                                                                                    |
| Data Classification         | Data classifications, outlined in the Information Security Policy, categorize Institutional Data based on the level of potential risk if the data were exposed. A data classification matrix is maintained that includes the security classification of the data and identifies a Steward and Custodian(s) for the data. Access to data will be granted based on these classifications and the role and job requirements of the requester. It is possible for data to be combined or gathered in specific ways that reveal information that might become sensitive in aggregate. |
| Data Collection and Maintenance | Ensuring the accuracy and quality of data (access control, backup, etc.) and implementing programs for data quality improvement.  

- Developing procedures for standardizing code values and coordinating maintenance of look-up tables used for Institutional Data.  
- Consulting with data consumers / users to determine appropriate data sources  
- Determining update precedence when multiple sources for data exist. |
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Lifecycle and Retention</td>
<td>Ensuring appropriate generation, use, retention, disposal, etc., of data and information consistent with University Policies, among them the Information Security Policy and standards for disposal.</td>
</tr>
</tbody>
</table>
| Data management              | Ensuring policies and procedures that manage Institutional Data as a University resource are established and these are communicated to the University community by the Data Stewards. These policies and procedures should include:  
  • Specific goals, objectives, and action plans to implement the policy and monitor progress in its implementation  
  • Identification of data entities and data sources that comprise Institutional Data and maintaining these entries in the IT Service Knowledge Management System or as Configuration Items in a Configuration Management Database. As this is an ongoing process there needs to be a regular and at least annual review of entries  
  • Prioritized management of Institutional Data including identifying – in consultation with relevant consumers and users of the data – which data is most critical and assigning appropriate management priorities to all data entities and sources  
  • Acceptable delivery modes for transmitting Institutional Data |
| Data Protection Act          | This DGSG policy is underpinned by the university’s commitment to complying with the Data Protection Act 1998 and the 8 Data Protection Principles, which are:-  
  • Personal data shall be processed fairly and lawfully.  
  • Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.  
  • Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.  
  • Personal data shall be accurate and, where necessary, kept up to date.  
  • Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.  
  • Personal data shall be processed in accordance with the rights of data subjects under this Act.  
  • Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.  
  • Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. |
| Data Quality, Integrity, and Correction | Ensuring proper use of Institutional Data and recommending appropriate policies regarding the manipulation or reporting of Institutional Data elements (in line with reporting standards established by the ITGS and DGSG) and implementing business unit procedures to carry out these policies. |
| Data Storage                 | Documenting official storage locations, archiving and retention requirements for data elements.                                               |
| Data User                    | Data Users are everyone who access Institutional data in performance of their assigned duties (Students, Researchers, Staff, Affiliates and Third Parties with access to University Data)  
Consumers / Users are employees or agents of the University who access Institutional Data in performance of their assigned duties. This access includes reading, entering, downloading, copying, querying, analysing, or updating data or information. |
| Education (Training and Advice) | Ensuring that education of employees responsible for managing the data is provided in reporting standards, data retention, data handling, and data security. |
Institutional Data Governance Policy

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institutional Data Model</td>
<td>Ensuring the creation and maintenance of an Institutional Data model and defining the standard for documentation of data elements. This includes definition and documentation of data entities, data flows between systems and organisations so that the origin of data elements can be traced through the organisational systems and processes.</td>
</tr>
</tbody>
</table>
| Institutional Data | Data that is created, acquired, or maintained by University employees in performance of official administrative job duties. Institutional Data is a subset of the University’s information resources and administrative records and includes any information in print, electronic, or audio-visual format that meets the following criteria:  
  - Acquired or maintained by university employees in performing their job duties;  
  - Relevant to planning, managing, operating, or auditing a major function at the university;  
  - Created, referenced or required for use by more than one organizational unit;  
  - Included in official University administrative reports or official university records |
| Record             | Data or information in a fixed form that is created or received in the course of individual or institutional activity and set aside (preserved) as evidence of that activity for future reference |

Appendix: King’s Principles for Data Governance and Decision Support

King’s ITGS Principles on Sharepoint

A number of Governing and Architectural Principles apply to Data Governance and Decision Support. These are listed below:

Cover the University end-to-end - Governing Principle 2

Architectural Principles

- Deliver Benefit to the University – Architecture Principle
- Business Continuity - Architecture Principle
- Common Use Applications – Architecture Principle
- Data is an Asset - Architecture Principle
- Data that has shared value should be shared - Architecture Principle
- Data is Accessible - Architecture Principle
- Data Trustee - Architecture Principle
- Common Vocabulary and Data Definitions – Architecture Principle
- Data Security - Architecture Principle
- Design Factors - Architecture Principle
- Control Technical Diversity - Architecture Principle
- Interoperability - Architecture Principle

The following architecture principles are of particular relevance
### Institutional Data Governance Policy

<table>
<thead>
<tr>
<th>Name</th>
<th>Data is an Asset</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Statement</strong></td>
<td>Data is an asset that has value to the University and is managed accordingly</td>
</tr>
<tr>
<td><strong>Rationale</strong></td>
<td>Data is a valuable corporate resource; it has real, measurable value. In simple terms, the purpose of data is to aid decision-making. Accurate, timely data is critical to accurate, timely decisions. Most corporate assets are carefully managed, and data is no exception. Data is the foundation of our decision making, so we must also carefully manage data to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it. Auditability ensures that data integrity and transparency can be demonstrated for all data. Importance recognises that some data is more critical than other data and identifies the importance of the data so that appropriate controls exist for the data. It is necessary for data of critical importance to be treated differently from data of a trivial or unimportant nature. Data will be standardized insofar as it is possible to limit the number of processes, categorisations and treatments necessary.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Data that has shared value should be shared</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Statement</strong></td>
<td>Users have access to the data necessary to perform their duties; therefore, data is shared across University functions and organizations.</td>
</tr>
<tr>
<td><strong>Rationale</strong></td>
<td>Timely access to accurate data is essential to improving the quality and efficiency of University decision-making. It is less costly to maintain timely, accurate data in a single application, and then share it, than it is to maintain duplicative data in multiple applications. The University holds a wealth of data, but it is stored in hundreds of incompatible stovepipe databases. The speed of data collection, creation, transfer, and assimilation is driven by the ability of the organization to efficiently share these islands of data across the organization. Shared data will result in improved decisions since we will rely on fewer (ultimately one virtual) sources of more accurate and timely managed data for all of our decision-making. Electronically shared data will result in increased efficiency when existing data entities can be used, without re-keying, to create new entities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Data is Accessible</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Statement</strong></td>
<td>Data is accessible for users to perform their functions when and how they need it.</td>
</tr>
<tr>
<td><strong>Rationale</strong></td>
<td>Wide access to data leads to efficiency and effectiveness in decision-making, and affords timely response to information requests and service delivery. Using information must be considered from a University perspective to allow access by a wide variety of users. Staff time is saved and consistency of data is improved. Data transparency enables the origin of data to be identified and assured for integrity from the data source to the destination storage location at all times.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Data Trustee or Stewardship</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Statement</strong></td>
<td>Each core University data domain has a trustee accountable for data quality.</td>
</tr>
<tr>
<td><strong>Rationale</strong></td>
<td>One of the benefits of an architected environment is the ability to share data (e.g., text, video, sound, etc.) across the University. As the degree of data sharing grows and business units rely upon common information, it becomes essential that only the data trustee makes decisions about the content of data. Data integrity should be preserved through storage, retrieval, manipulation, transformation, replication and maintenance activities. Since data loses its integrity when it is entered multiple times, cost of ownership is multiplied and decision support is compromised, the data trustee will have sole responsibility for data entry which eliminates redundant human effort and data storage resources. Stewardship ensures there is accountability for stewardship activities by individual data contributor and groups of Data Stewards. Accountabilities ensures there is identified ownership of data elements and data sets. Checks and balances are needed on an on-going basis to actively identify areas for improvement and to adherence to Data Governance. This reduces the likelihood of a single person being able to inadvertently or wilfully breach this policy.</td>
</tr>
</tbody>
</table>
### Common Vocabulary and Data Definitions

**Statement**
Data is defined consistently throughout the University, and the definitions are understandable and available to all users.

**Rationale**
The data that will be used in the development of applications must have a common definition throughout the Headquarters to enable sharing of data. A common vocabulary will facilitate communications and enable dialogue to be effective. In addition, it is required to interface systems and exchange data.

### Data Security

**Statement**
Data, whether stored, in transit or in use, is protected from unauthorized use and disclosure to ensure the required levels of confidentiality, integrity and accessibility.

**Secure yet Pragmatic** (Be secure whilst not over-complicating what we have)

**Rationale**
Data Security is subject to external regulation and compliance. Fines must be avoided and University reputation protected.

Like any asset, data must be protected and secure (preserving confidentiality, integrity and accessibility). A major part of a University’s Intellectual Property (IP) is hosted in the IT domain. The University’s IP must be protected. This protection must be reflected in the IT architecture, implementation, and governance processes. University data must be safeguarded against inadvertent or unauthorized alteration, sabotage, disaster, or disclosure.

Designs for security solutions should be as simple as is needed to make them effective and be coherent across the whole architecture. Unnecessary complexity is a threat to performance, maintainability and good security. A complex security system solution increases the likelihood of unknown and unforeseen weaknesses in its security, and makes it more difficult to understand. A solution cannot be protected sufficiently if it is not sufficiently understood and easy to manage. Secure architectures are most effective when based on a thorough understanding of the requirements, leading to a design that provides effective adequate protection while minimizing complexity and impact on operational performance.

### Interoperability

**Statement**
Interoperable (Ensure what we have works well together). Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology.

**Rationale**
Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing IT investments, thus maximizing return on investment and reducing costs. Standards for interoperability additionally help ensure support from multiple vendors for their products, and facilitate supply chain integration.

We adapt and apply best practice, proven technology and ways of working to work for Kings.